Security Risk Management and Assessment

Security Risk Analysis for

Bright Smile Dental Group (Fictional Entity)

Assessment conducted by **En Ci Mong**

Under the Guidance of **Professor**

Date: December 8, 2025

Table of Contents

Part A- Security Risk Management Assessment for Hypothetical Governmental Agency

(III) Executive Summary

Information System Categorization:

	Confidentiality (C)	Integrity (I)	Availability (A)
Payroll System & Financial Resources	H	H	H
Employee Master Database	H	H	H
Time and Attendance Application	H	H	M
HGA Reputation & Public Trust	M	L	L

Organization Name: Hypothetical government agency (HGA)

Organization Address: 123 Liberty Plaza, Washington, D.C. 20004

Organization Senior Management List

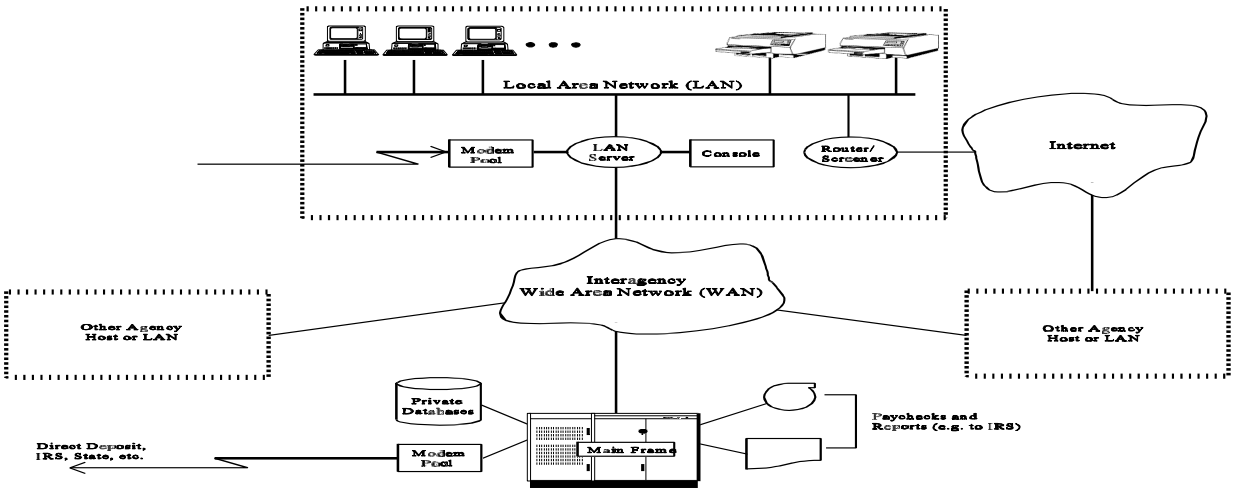
Name: Steven Cook
Title: Chief Executive Officer (CEO)
Email: Cook.S@gmail.com
Phone Number: +1 781-231-6648

Name: Emily Maldivian
Title: Chief Information Officer (CIO)
Email: Maldivine.E@gmail.com
Phone Number: +1 792-524-6391

Name: Mason Zywicki
Title: Chief Information Security Officer (CISO)
Email: Zywicki.M@gmail.com
Phone Number: +1 793-873-0083

Name: Taylor Huang
Title: Chief Financial Officer (CFO)
Email: Huang.T@gmail.com
Phone Number: +1 723-698-6190

Information system Operation Status: Operational/Production
Information System Type: Distributed LAN (Local Area Network)System, transaction processing systems



System Description:

- HGA operates a distributed computer system that processes time and attendance data for federal payroll operations. The system manages sensitive personnel information, including salary data, leave balances, W-2 records, and service dates for agency employees. Our infrastructure consists of personal computers connected through a local area network to a central server that enforces access controls, provides file storage, hosts email services, and executes applications. Time and attendance data entered on workstations undergoes validation on the server before transmission through an inter-agency wide area network to a shared mainframe for payroll processing and electronic funds distribution. The system connects to three external networks: the Internet through a packet-filtering router (email only), an X.25-based inter-agency WAN (authorized applications only), and the public telephone network via modem pool (email access for remote users). Additional capabilities include word processing, data analysis, electronic communications, and management of personnel correspondence and contracting documents.

System Topology:

- The system follows a three-tier distributed architecture with mixed ownership. The first tier includes our personal computers with local storage and network printers; all connected through the LAN backbone within our security perimeter. The second tier comprises our edge infrastructure: a central LAN server that serves as the primary security enforcement point, an administrator console for privileged system management, a modem pool for remote access, and a router providing filtered Internet connectivity. The third tier consists of external systems beyond our direct control, including the X.25 WAN operated by a commercial telecommunications provider and a multi-agency mainframe owned by another federal agency. The mainframe houses payroll databases and includes its own modem pool for electronic funds transfer. Time and attendance data flows from workstations through our server, across the WAN, to the mainframe, where it generates direct deposits, paychecks, and tax reporting to IRS and state agencies.

Critical Path for Time and Attendance Processing:

- User PC (data entry) → LAN Server (validation and access control enforcement) → WAN Interface (secure transmission) → X.25 Wide Area Network (inter-agency transport) → Mainframe System (payroll processing and database storage) → Electronic Distribution (direct deposits to employee bank accounts, paychecks, and tax reports to IRS/state agencies)

System Name: HGA Time and Attendance Processing System

Type of Organization: Federal Government Agency

Type of Agreement: Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU) with commercial telecommunications provider for WAN services and separate federal agency for mainframe payroll processing services

Establishment Date: 21April,1981

NIST FIPS 199 Category: High

CA Status: Authorization to Operate (ATO)

Authorizing Official: Steven Cook (CEO)

List of Applicable Law, Policies, Framework, Standards, and Regulations:

- **NIST 800-53:Security and Privacy Controls for Federal Information System and Organization.**
- **ISO/IEC 27001:Information Security Management System (ISMS)**
- **General Data Protection Regulation(GDPR)**
- **Data Protection Act (DPA)**
- **Computer Fraud and Abuse Act (CFAA)**
- **Gramma-Leach-Billey Act (GBLA)**
- **Federal Risk and Authorization Management Program (FedRAMP) – For any Government agencies using cloud services**
- **Federal Information and Security Management Act (FISMA)**

Security Control	Observation	Status	Control Type	Responsible Authority
Access Control (AC)	User access rights managed through role-based permissions; privileged access monitored	Implemented	Common	CIO
Awareness and Training (AT)	Annual security awareness training completed; role-based training for system administrators	Partially Implemented	Common	CISO
Audit and Accountability (AU)	Centralized logging enabled; audit records retained per policy; regular log reviews conducted	Implemented	Common	CISO
Assessment, Authorization, and Monitoring (CA)	Annual security assessments performed; continuous monitoring program active	Implemented	Common	CISO
Configuration Management (CM)	Baseline configurations documented; change control process established	Partially Implemented	Common	CISO

Contingency Planning (CP)	Business continuity plan documented; backup procedures tested quarterly	Partially Implemented	Common	CIO
Identification and Authentication (IA)	Multi-factor authentication deployed for privileged users; password policies enforced	Implemented	Common	CISO
Incident Response (IR)	Incident response plan established; team trained and contact lists maintained	Partially Implemented	Common	CISO
Maintenance (MA)	Scheduled maintenance windows defined; maintenance activities logged	Implemented	Common	CISO
Media Protection (MP)	Media sanitization procedures documented; encryption used for portable media	Partially Implemented	Common	CIO
Physics and Environmental Protection (PE)	Physical access controls in place; environmental monitoring systems active	Implemented	Common	CISO
Planning (PL)	System security plans documented and approved; security architecture documented	Implemented	Common	CIO
Program Management (PM)	Security program strategy documented; resources allocated per risk priorities	Partially Implemented	Common	CIO
Personnel Security (PS)	Background checks completed; termination procedures established	Implemented	Common	CISO
Personally Identifiable Information Processing and Transparency (PT)	PII inventory maintained; privacy impact assessments conducted	Partially Implemented	Common	CISO
Risk Assessment (RA)	Annual risk assessments conducted; threat intelligence reviewed regularly	Implemented	Common	CISO
System and Services Acquisition (SA)	Security requirements included in procurement; vendor assessments performed	Partially Implemented	Common	CIO
System and Communications Protection (SC)	Network segmentation implemented; encryption in transit and at rest enabled	Implemented	Common	CISO

System and Information Integrity (SI)	Vulnerability scanning automated; patch management process operational	Partially Implemented	Common	CISO
Supply Chain Risk Management (SR)	Supply chain risk assessments conducted; SBOMs reviewed for critical systems	Partially Implemented	Common	CISO

Information Security Plan Completion Date: 12-1-2025

Information Security Approval Date: 12- 8-2025

(IV) List of Assets with Values ($):

- **Total Value for HGA Assets is $3,045,000 or $3.04M**

Asset Number	Asset Name	Description	Asset Value
A1	Payroll System & Financial Resources	Critical system managing US Government fund transfers including paychecks, direct deposits, and tax withholdings. Financial integrity essential to agency mission and employee welfare.	**800000**
A2	Employee Master Database	Comprehensive personnel database stored on mainframe containing service dates, leave balances, salary information, W-2 data, and other Privacy Act protected information.	**600000**
A3	Time and Attendance Application	Weekly timesheet processing system including data entry, validation, supervisor approval, and mainframe submission. Core component of payroll fraud prevention.	**400000**
A4	Personnel Information & Records	Employment records, background investigations, performance evaluations, correspondence, and other human resources data requiring confidentiality protection.	**300000**
A5	Draft Regulations & Policy Documents	Pre-publication regulatory documents and internal policy drafts with potential competitive and policy implications if prematurely disclosed.	**100000**
A6	LAN Server Infrastructure	Central processing platform providing shared storage, application execution, email services, and network connectivity for distributed operations.	**90000**
A7	Contracting & Procurement Documents	Vendor agreements, pricing information, procurement strategies, and competitive bidding documents with financial sensitivity.	**85000**
A8	Network Infrastructure (Router/WAN)	Communication equipment including Internet router, WAN connection, and packet filtering systems enabling external connectivity.	**70000**
A9	Personal Computer Workstations	Individual desktop systems with local storage, processing capability, and network connectivity distributed throughout agency facilities.	**50000**

A10	Internal Business Communications	Inter-departmental correspondence, meeting records, administrative memos, and routine business documentation.	**50000**
A11	HGA Reputation & Public Trust	Agency credibility with Congress, citizens, and other federal agencies. Intangible but mission-critical asset affecting operational effectiveness.	**500000**

(V) List of threats

Threat ID	Threat Name	Description
T1	Payroll Fraud	Fraudulent timesheet submission for unworked hours, falsifying service dates for retirement benefits, creating fictitious employee records. Historical attempts primarily from within HGA.
T2	Payroll Errors	Data entry mistakes, failure to process personnel changes timely, accidental corruption of time and attendance data, inter-agency coordination failures.
T3	In Interruption of Operations	Unauthorized access to employee databases for Power outages from aging infrastructure, equipment malfunctions, natural disasters, malicious disruption targeting time-critical payroll processing.
T4	Information Disclosure/Brokerage	Legitimate users accessing employee database to sell information to private investigators, employment recruiters, press for commercial gain.
T5	Network-Related Threats	External penetration via Internet, password guessing, unauthorized dial-up access, exploitation of email utility bugs for administrator privileges.
T6	Accidental Loss/Release of Information	Unintentional exposure of disclosure-sensitive personnel data through poor handling, unsecured storage, inadvertent transmission.
T7	Theft	Physical theft of computer equipment, storage media, documents containing sensitive information from agency facilities.
T8	Virus Contamination	Malware infections causing data corruption, system disruption, unauthorized access through infected software or removable media.
T9	Natural Disaster	Fires, floods, storms causing extended outages and data loss affecting critical business operations.
T10	Unauthorized Telecommunications Access	Eavesdropping on dial-up connections, WAN communications, modem pool exploitation for unauthorized system access.

(VI)List of Security Vulnerabilities

Vulnerability ID	Vulnerability Name	Description

V1	Clear-text Password Transmission	User passwords broadcast unencrypted over LAN during authentication, easily captured by network sniffing tools or malicious software.
V2	Immature Server Operating System	LAN server uses recently deployed OS with known security vulnerabilities and insufficient hardening against privilege escalation attacks.
V3	Inadequate Physical Security Compliance	Widespread non-compliance with document storage policies, unlocked computers containing sensitive data, and poor after-hours security practices.
V4	Email System File Access Vulnerability	Email utility allows users to attach any accessible file to outgoing messages, enabling data exfiltration via Internet or dial-up connections.
V5	Weak Administrative Controls	Delayed security patch installation, insufficient compliance monitoring, and lack of regular security awareness training updates.
V6	Mainframe Authentication Weaknesses	Shared mainframe system relies on password-only authentication serving multiple agencies with varying security standards, creating attack vectors.
V7	WAN Data Interception	Time and attendance data transmitted over WAN vulnerable to tampering at relay switches, potential HGA-WAN provider collusion.
V8	Unencrypted LAN Communications	Information broadcast to all LAN connection points without encryption, trivial eavesdropping with widely available sniffer programs.
V9	Inadequate PC Backup Procedures	Many users store significant data locally without backing up, leading to frequent data loss incidents.
V10	Virus Prevention Non-compliance	COG personnel not routinely running virus scanners despite monthly requirements, only during publicized scares.
V11	Untested Contingency Plans	Alternative site processing capabilities never verified despite annual testing requirements, may prove illusory during emergencies.
V12	Insufficient Audit Logging	Systems lack capabilities to track attacker activities, cannot accurately gauge extent of network penetrations when they occur.

(VII) Threat/Vulnerability pairs (with probabilities 0%-100% that a threat will exploit the specific vulnerability

Asset Number	Asset Name	Description	Asset Value
A1	Payroll System & Financial Resources	Critical system managing US Government fund transfers including paychecks, direct deposits, and	**800000**

		tax withholdings. Financial integrity essential to agency mission and employee welfare.	
A2	Employee Master Database	Comprehensive personnel database stored on mainframe containing service dates, leave balances, salary information, W-2 data, and other Privacy Act protected information.	**600000**
A3	Time and Attendance Application	Weekly timesheet processing system including data entry, validation, supervisor approval, and mainframe submission. Core component of payroll fraud prevention.	**400000**
A11	HGA Reputation & Public Trust	Agency credibility with Congress, citizens, and other federal agencies. Intangible but mission-critical asset affecting operational effectiveness.	**500000**

Threat ID	Threat Name	Description
T1	Payroll Fraud	Fraudulent timesheet submission for unworked hours, falsifying service dates for retirement benefits, creating fictitious employee records. Historical attempts primarily from within HGA.
T3	Interruption of Operations	Power outages from aging infrastructure, equipment malfunctions, natural disasters, malicious disruption targeting time-critical payroll processing.
T4	Information Disclosure/Brokerage	Legitimate users accessing employee database to sell information to private investigators, employment recruiters, press for commercial gain.
T5	Network-Related Threats	External penetration via Internet, password guessing, unauthorized dial-up access, exploitation of email utility bugs for administrator privileges.

Vulnerability Number	Vulnerability Name	Description
V1	Clear-text Password Transmission	User passwords broadcast unencrypted over LAN during authentication, easily captured by network sniffing tools or malicious software.
V3	Inadequate Physical Security Compliance	Widespread non-compliance with document storage policies, unlocked computers containing sensitive data, and poor after-hours security practices.
V4	Email System File Access Vulnerability	Email utility allows users to attach any accessible file to outgoing messages, enabling data exfiltration via Internet or dial-up connections.
V11	Untested Contingency Plans	Alternative site processing capabilities never verified despite annual testing requirements, may prove illusory during emergencies.

- Threat/Vulnerability pairs with likelihood probabilities 0%-100%; provide a brief explanation of assigned probability values

T1, T3 exploits **V1** on assets **A1**, **A2** and **A3**

T4, T5 exploit **V3** on assets **A1, A2, A3, A11**

T4, T5 exploit **V4** on assets **A1, A2, A3, A11**

T3 exploits **V11** on assets **A1, A2, A3, A11**

	T1	**T3**	**T4**	**T5**
V1 on assets A1, A2 and A3	85%	85%	80%	80%
V3 on assets A1, A2, A3, A11	70%	75%	90%	90%
V4 on assets A1, A2, A3, A11	65%	70%	75%	75%
V11 on assets A1, A2, A3, A11	60%	80%	55%	60%

Threat-Asset Relationship Analysis

- **Payroll Fraud (T1)** achieves highest probability (85%) when exploiting clear-text password transmission (V1) on A1 (Payroll System & Financial Resources), A2 (Employee Master Database), and A3 (Time & Attendance Application). Historical fraud attempts documented at HGA combined with easily intercepted authentication credentials create direct pathways for unauthorized government fund transfers and fictitious employee creation. Physical security non-compliance (V3) provides 70% probability for insider fraud through after-hours system access, while email vulnerabilities (V4) at 65% and untested contingency plans (V11) at 60% offer additional but less direct fraud opportunities requiring more sophisticated attack coordination.
- **Interruption of Operations (T3)** shows highest impact probability (85%) through password interception (V1) enabling external attackers to disrupt critical payroll processing systems, particularly affecting time-sensitive operations across A1, A2, and A3. Untested contingency plans (V11) create 80% probability of extended outages due to HGA's aging infrastructure and never-verified recovery procedures. Physical security failures (V3) at 75% enable deliberate system disruption by malicious insiders, while email system exploitation (V4) at 70% can interrupt communications essential for coordinating time-critical payroll deadlines across all affected assets including A11 reputation damage.

- **Information Disclosure/Brokerage (T4)** reaches maximum probability (90%) through physical security non-compliance (V3) affecting all critical assets A1, A2, A3, and A11, reflecting widespread policy violations including unlocked computers and unsecured documents that enable after-hours personnel data theft for commercial sale. Clear-text password transmission (V1) provides 80% probability for database access by information brokers, while email vulnerabilities (V4) at 75% facilitate large-scale data exfiltration to external parties. Untested contingency plans (V11) show lowest probability (55%) as recovery failures don't directly enable information brokerage but create opportunities during emergency periods when security controls are relaxed.

- **Network-Related Threats (T5)** mirror T4 probabilities with physical security failures (V3) at 90% enabling external actors to gain internal network access through direct console manipulation and malicious software installation. Password interception vulnerabilities (V1) provide 80% probability for external penetration attempts documented annually at HGA, while email system bugs (V4) at

75% have historical precedent including one case where attackers gained System Administrator privileges. Contingency plan failures (V11) at 60% create moderate risk during system outages when network security controls may be degraded, requiring coordination with actual infrastructure failures to maximize exploitation success.

(VIII) Asset/Vulnerability pairs for Critical Assets included in the subset for only the Vulnerabilities present on each Critical Asset (Assets impacted by Threat/Vulnerability pairs)

Asset Number & Name	**Vulnerability Number & Name**	**Vulnerability Description**
A1: Payroll System	V1: Clear-text Password Transmission	User passwords broadcast unencrypted over LAN during authentication, easily captured by network sniffing tools or malicious software.
	V3: Inadequate Physical Security Compliance	Widespread non-compliance with document storage policies, unlocked computers containing sensitive data, and poor after-hours security practices.
	V4: Email System File Access Vulnerability	Email utility allows users to attach any accessible file to outgoing messages, enabling data exfiltration via Internet or dial-up connections.
	V11: Untested Contingency Plans	Alternative site processing capabilities never verified despite annual testing requirements, may prove illusory during emergencies.
A2: Employee Master Database	V1: Clear-text Password Transmission	User passwords broadcast unencrypted over LAN during authentication, easily captured by network sniffing tools or malicious software.
	V3: Inadequate Physical Security Compliance	Widespread non-compliance with document storage policies, unlocked computers containing sensitive data, and poor after-hours security practices.
	V4: Email System File Access Vulnerability	Email utility allows users to attach any accessible file to outgoing messages, enabling data exfiltration via Internet or dial-up connections.
	V11: Untested Contingency Plans	Alternative site processing capabilities never verified despite annual testing requirements, may prove illusory during emergencies.
A3: Time & Attendance Application	V1: Clear-text Password Transmission	User passwords broadcast unencrypted over LAN during authentication, easily captured by network sniffing tools or malicious software.
	V3: Inadequate Physical Security Compliance	Widespread non-compliance with document storage policies, unlocked computers containing sensitive data, and poor after-hours security practices.
	V4: Email System File Access Vulnerability	Email utility allows users to attach any accessible file to outgoing messages, enabling data exfiltration via Internet or dial-up connections.
	V11: Untested Contingency Plans	Alternative site processing capabilities never verified despite annual testing requirements, may prove illusory during emergencies.

A11: HGA Reputation	V3: Inadequate Physical Security Compliance	Widespread non-compliance with document storage policies, unlocked computers containing sensitive data, and poor after-hours security practices.
	V4: Email System File Access Vulnerability	Email utility allows users to attach any accessible file to outgoing messages, enabling data exfiltration via Internet or dial-up connections.
	V11: Untested Contingency Plans	Alternative site processing capabilities never verified despite annual testing requirements, may prove illusory during emergencies.

- Initial Risk Impacts: if a Threat/Vulnerability pair exists on a critical Asset, then100%, therefore 0% Resilience, which is worst case scenario

Risk Impact (RI) Table																
Assets	**T1* V1**	**T1* V3**	**T1* V4**	**T1* V11**	**T3* V1**	**T3* V3**	**T3* V4**	**T3* V11**	**T4* V1**	**T4* V3**	**T4* V4**	**T4* V11**	**T5* V1**	**T5* V3**	**T5* V4**	**T5* V11**
A1	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A2	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A3	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100	100
A11	0	100	100	100	0	100	100	100	0	100	100	100	0	100	100	100

Explanation:

- **0% Impact for V1 (Password) Combinations:** Clear-text password transmission is an internal technical vulnerability. Stakeholders (Congress, citizens, federal agencies) cannot directly observe authentication protocols. Password weaknesses only damage reputation if they enable visible security incidents - the vulnerability itself remains invisible.
- **100% Impact for V3, V4, V11 Combinations:V3 (**Inadequate Physical Security Compliance**)** Policy violations create visible data breaches that generate Congressional hearings and media coverage.**V4 (**Email System File Access Vulnerability**)**Enables public data leaks and Privacy Act violations that immediately harm public trust.**V11 (**Untested Contingency Plans)Causes extended payroll outages that create employee complaints and operational credibility loss.

(IX) MOT-Which MOT controls are covered by current HGA controls (Histogram)

Management	**Operational**	**Technical**
Policies **(M1)**	Personnel/User Issues **(M6)**	Identification and Authentication **(M12)**
Program Management **(M2)**	Preparing for Contingencies and Disasters **(M7)**	Logical Access Control **(M13)**
Risk Management **(M3)**	Incident Reporting and Handling **(M8)**	Audit Trails **(M14)**
Life Cycle Planning **(M4)**	Awareness, Training and Education **(M9)**	Cryptography **(M15)**

Assurance **(M5)**	Security Considerations in Support and Operations **(M10)**	
	Physical and Environmental Security **(M11)**	

Current security controls and policies (CSCP):

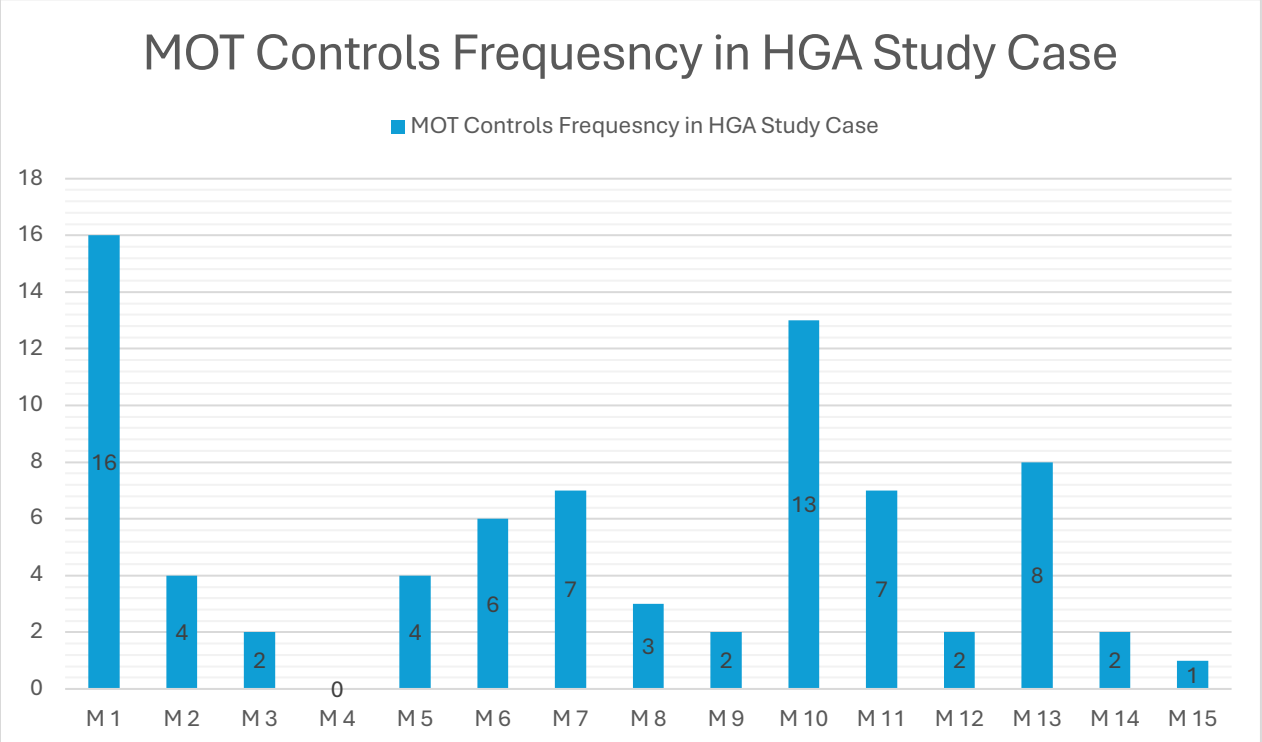
CSCP Number	Category	Description	MOT Controls
CSCP1	General Purpose	Computer Security Manual implementing OMB A-130, Computer Security Act of 1987, Privacy Act, OMB A-123/A-127, Federal Managers' Financial Integrity Act	**M1, M2**
CSCP2	General Purpose	Need-to-know access policy limiting information access to job requirements only	**M1, M6**
CSCP3	General Purpose	Written authorization required from department supervisors before system access	**M1, M6**
CSCP4	General Purpose	Mandatory security awareness training before account activation	**M9**
CSCP5	General Purpose	Acknowledgment forms requiring users to understand security responsibilities	**M6, M9**
CSCP6	General Purpose	Background investigations and personnel screening procedures	**M6**
CSCP7	General Purpose	Only System Administrators authorized to establish login IDs and passwords	**M6, M10**
CSCP8	General Purpose	Password selection and periodic change requirements with penalties for non-compliance	**M1, M12**
CSCP9	Protection Against Unauthorized Execution	Separation of duties requiring two-person approval for payroll transactions	**M1, M6**
CSCP10	Protection Against Unauthorized Execution	LAN server elementary access control lists limiting file and program access	**M13**
CSCP11	Protection Against Unauthorized Execution	Group-oriented controls allowing team-based access to sensitive files	**M13**
CSCP12	Protection Against Unauthorized Execution	Password-based identification and authentication for server access	**M12**

CSCP13	Protection Against Unauthorized Execution	Special access control privileges required for WAN interface access	**M13**
CSCP14	Protection Against Unauthorized Execution	Time and attendance application restricted to specific PCs and business hours	**M13**
CSCP15	Protection Against Payroll Errors	Automated data validation checking for invalid employee IDs and implausible hours	**M5, M10**
CSCP16	Protection Against Payroll Errors	Dual data entry system for time sheets with discrepancy detection	**M5, M10**
CSCP17	Protection Against Payroll Errors	Weekly paper timesheet submission with supervisor approval	**M1, M6**
CSCP18	Protection Against Payroll Errors	Exception reporting for negative leave balances and out-of-range values	**M10, M14**
CSCP19	Protection Against Payroll Errors	Personnel action forms required one week before payroll processing	**M1, M10**
CSCP20	Protection Against Accidental Corruption or Loss of Payroll Data	Nightly server disk backups to magnetic tape with weekly offsite storage	**M7, M10**
CSCP21	Protection Against Accidental Corruption or Loss of Payroll Data	One-year online retention with three-year archive for time and attendance data	**M13**
CSCP22	Protection Against Accidental Corruption or Loss of Payroll Data	Read-only access automatically set for submitted payroll files	**M13**
CSCP23	Protection Against Accidental Corruption or Loss of Payroll Data	WAN communications protocols with error checking for data transmission	**M5, M15**
CSCP24	Protection Against Accidental	Pre-payroll validation reports identifying missing agency data	**M10, M14**

	Corruption or Loss of Payroll Data		
CSCP25	Protection Against Interruption of Operations	Computer Operations Group (COG) responsible for system management	**M2, M10**
CSCP26	Protection Against Interruption of Operations	Spare equipment inventory (10 PCs, spare server, disk drives, LAN cable)	**M7, M11**
CSCP27	Protection Against Interruption of Operations	Emergency LAN cabling procedures for severed connections	**M7, M10**
CSCP28	Protection Against Interruption of Operations	Controlled software installation (COG-approved licensed packages only)	**M1, M10**
CSCP29	Protection Against Interruption of Operations	Monthly virus scanning requirements with incident reporting	**M8, M10**
CSCP30	Protection Against Interruption of Operations	Annual contingency plan testing requirements	**M7**
CSCP31	Protection Against Interruption of Operations	Alternative site agreements with nearby agencies for emergency operations	**M7**
CSCP32	Protection Against Interruption of Operations	Application priority procedures for degraded capacity situations	**M1, M7**
CSCP33	Protection Against Interruption of Operations	Backup service capacity for 100+ simultaneous users	**M7, M11**
CSCP34	Protection Against Disclosure or Brokerage of Information	Mandatory locked file cabinet/drawer storage for sensitive papers	**M1, M11**
CSCP35	Protection Against Disclosure or Brokerage of Information	PC key locks installed on all computers with locking requirements	**M11**

CSCP36	Protection Against Disclosure or Brokerage of Information	Office locking requirements for overnight protection	**M1, M11**
CSCP37	Protection Against Disclosure or Brokerage of Information	Approved storage containers with key control limited to document owners	**M1, M11**
CSCP38	Protection Against Disclosure or Brokerage of	Building security with guard force access controls	**M11**
CSCP39	Protection Against Disclosure or Brokerage of Information	Server audit log review by COG with security violation reporting	**M8, M14**
CSCP40	Protection Against Network-Related Threats	Router packet filtering allowing only email traffic between LAN and Internet	**M13**
CSCP41	Protection Against Network-Related Threats	Dial-up access restricted to email functions only	**M13**
CSCP42	Protection Against Network-Related Threats	Administrator console exclusive access for server configuration	**M11, M13**
CSCP43	Protection Against Network-Related Threats	Incident Handling Team for security breach coordination	**M2, M8**
CSCP44	Protection Against Network-Related Threats	Vendor security patch installation procedures	**M10**
CSCP45	Protection Against Network-Related Threats	Security configuration validation utilities	**M5, M10**

CSCP46	Protection Against Risks from Non-HGA Computer Systems	External system authorization required from application owner and COG Manager	**M1, M2**
CSCP47	Protection Against Risks from Non-HGA Computer Systems	Written safeguarding commitments required from controlling organizations	**M1, M3**
CSCP48	Protection Against Risks from Non-HGA Computer Systems	Internet usage policy allowing email but prohibiting proprietary data transmission	**M1**
CSCP49	Protection Against Risks from Non-HGA Computer Systems	Information protection requirements commensurate with HGA-designated value	**M1, M3**

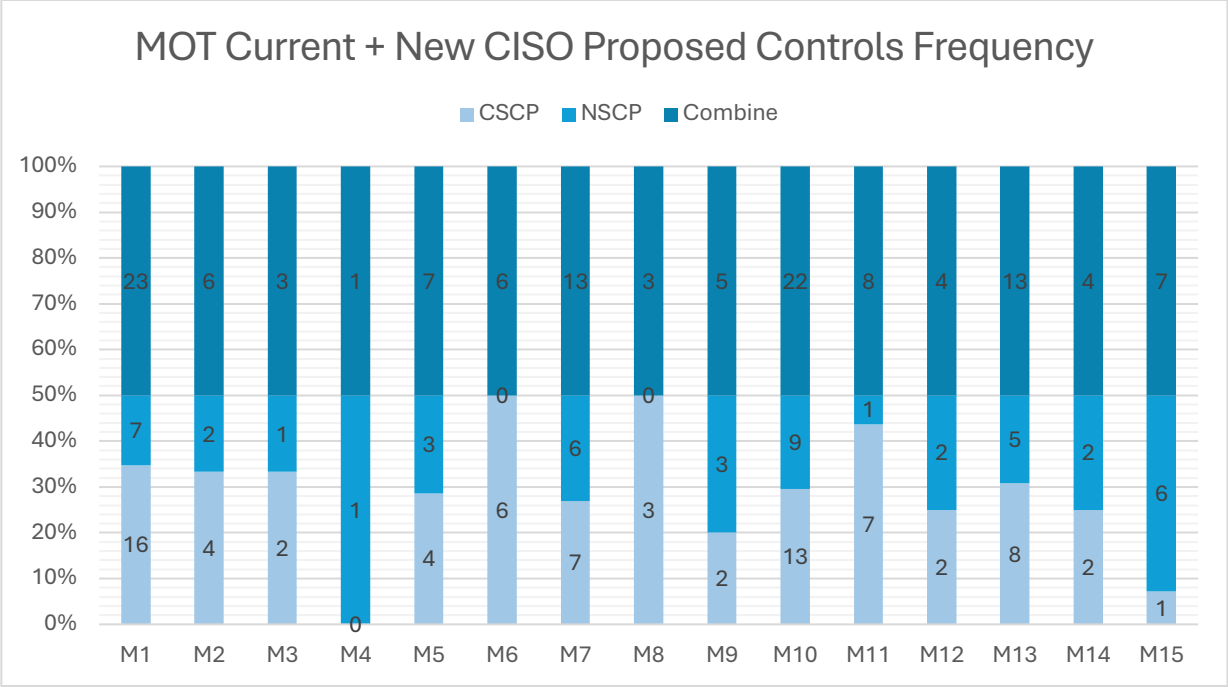


(X) MOT-Which MOT controls are covered by current AND proposed by new CISO HGA controls AND VPN server AND DMZ (Histogram)

List of New Security Controls and Policies (NSCP)

NSCP Number	Category	Description	MOT Controls
NSCP1	Payroll Fraud Mitigation	One-time password system using programmable smart tokens for Time and Attendance Clerks and Supervisors	**M12**
NSCP2	Payroll Fraud Mitigation	Public key cryptographic signatures for time and attendance data	**M15**
NSCP3	Payroll Fraud Mitigation	Improved monitoring of LAN server's access control configuration	**M10, M13**
NSCP4	Payroll Fraud Mitigation	Management decision to maintain current supervisory review procedures	**M1, M13**
NSCP5	Payroll Error Mitigation	Regular audits of paperwork handling procedures	**M5, M10**
NSCP6	Payroll Error Mitigation	Enhanced compliance framework with defined consequences	**M1, M2**
NSCP7	Payroll Error Mitigation	Secondary benefit of digital signature system	**M5, M15**
NSCP8	Continuity of Operations	Periodic internal training for COG personnel	**M7, M9**
NSCP9	Continuity of Operations	Mandatory testing of emergency procedures	**M7**
NSCP10	Continuity of Operations	Alternative processing using magnetic tape	**M7**
NSCP11	Continuity of Operations	High-level review of mainframe contingency plans	**M2, M7**
NSCP12	Continuity of Operations	Enhanced compliance with existing virus prevention procedures	**M1, M10**
NSCP13	Continuity of Operations	Quarterly email reminders for PC users	**M9, M10**
NSCP14	Continuity of Operations	Regular backup for critical PCs	**M7, M10**
NSCP15	Information Disclosure/Brokerage Mitigation	Mandatory refresher courses with compliance audits	**M5, M9**

NSCP16	Information Disclosure/Brokerage Mitigation	Automatic PC locking after idle periods	**M13**
NSCP17	Information Disclosure/Brokerage Mitigation	Requirement to store sensitive data on local hard disks only	**M1, M10**
NSCP18	Information Disclosure/Brokerage Mitigation	Enhanced monitoring and regular review of server access	**M10, M14**
NSCP19	Information Disclosure/Brokerage Mitigation	Personnel action forms required one week before payroll processing	**M1, M10**
NSCP20	Information Disclosure/Brokerage Mitigation	Protection for information on unattended PCs	**M15**
NSCP21	Information Disclosure/Brokerage Mitigation	Investigation of server-side encryption capabilities	**M4, M15**
NSCP22	Information Disclosure/Brokerage Mitigation	Regular review of mainframe access records	**M14**
NSCP23	Network-Related Threats Mitigation	Prohibition of sensitive information transmission outside HGA	**M1**
NSCP24	Network-Related Threats Mitigation	Enhanced restrictions for remote access	**M1, M13**
NSCP25	Network-Related Threats Mitigation	Alternative email system for dial-in users	**M10, M13**
NSCP26	Network-Related Threats Mitigation	Replacement of current modem pool	**M11, M15**
NSCP27	Network-Related Threats Mitigation	Encryption for server-to-mainframe communications	**M15**
NSCP28	Network-Related Threats Mitigation	Enhanced authentication for remote access	**M12**



(XI) Optimized Security Risk Prevention Strategy

Security Risk ($) calculations by implementing proposed controls by new CISO, missing MOT controls, 2-Factor Authentication, VPN and DMZ. Estimate a Risk Prevention budget. Compare the list of current HGA controls plus CISO proposed prevention controls plus missing MOT prevention controls plus 2-Factor Authentication, VPN and DMZ risk controls to the 178 risk controls from Common Criteria.

Proposed Controls:

- **New CISO**
- **Missing MOT Controls**
- **2-Factor Authentication**
- **VPN**
- **DMZ**

Risk Prevention Budget: $520000

VPN (Link):

- NordVPN's business option, NordLayer, starts at $10 per month (and $8 per month when paid annually)
- https://www.forbes.com/advisor/business/software/vpn-cost/

2FA(Link):

- $6 per user per month
- https://duo.com/editions-and-pricing (DUO)

	T1	T3	T4	T5
V1 on assets A1, A2 and A3	55%	65%	50%	60%

V3 on assets A1, A2, A3, A11	**40%**	**35%**	**30%**	**45%**
V4 on assets A1, A2, A3, A11	45%	40%	55%	45%
V11 on assets A1, A2, A3, A11	40%	50%	35%	30%

Residual Asset Security Risk:

Risk of Assets A1:
800000 * (230%+**150%**+185%+155%)/100% = $5,760,000 or $5.76M

Risk of Assets A2:
600000 * (230%+**150%**+185%+155%)/100% = $4,320,000 or $4.32M

Risk of Assets A3:
400000 * (230%+**150%**+185%+155%)/100% = $2,880,000 or $2.88M

Risk of Assets A11:
500000 * (**150%**+185%+155%)/100% = $2,450,000 or $2.45M

Residual Vulnerability Security Risk:

Risk For V1: [(800000 * 230%) + (600000 * 230%) + (400000 * 230%)] / 100 = $4,140,000 or $4.14M
Risk For **V3:** [(800000 * 150%) + (600000 * 150%) + (400000 * 150%) + (500000 * 150%)] / 100 = $3,450,000 or $3.45M
Risk For V4: [(800000* 185%) + (600000 * 185%) + (400000* 185%) + (500000 * 185%)] / 100 = $4,255,000 or $4.25M
Risk For V11: [(800000* 155%) + (600000 * 155%) + (400000 * 155%) + (500000 * 155%)] / 100 = $3,565,000 or $3.56M

Ranking of Security Asset Residual Risks:

Asset	Residual Security Risk	Ranking
A1	$5.76M	1
A2	$4.32M	2
A3	$2.88M	3
A11	$2.45M	4

Ranking of Vulnerability Security Risks:

Asset	Residual Security Risk	Ranking
V1	$4.14M	2
V3	$3.45M	4
V4	$4.25M	1
V11	$3.56M	3

(XII)Security Risk Response (Resilience) Strategy

Security Risk ($) calculations by implementing proposed controls by new CISO, missing MOT controls, Redundant Server and Mirror Site. Estimate a Risk Response budget. Compare the list of current HGA controls plus CISO proposed prevention controls plus missing MOT prevention controls plus Redundant Server and Mirror Site risk controls to the 178 risk controls from Common Criteria

Proposed Controls:

- **New CISO**
- **Missing MOT Controls**
- **Redundant Server**
- **Mirror Site**

Risk Prevention Budget: $750,000

Redundant Server (Link):

- $5000 ++
- https://www.itsasap.com/blog/server-cost

Mirror Site (Link):

- $300,000 Annually (Hot site)
- https://1111systems.com/blog/are-you-prepared-when-a-disaster-happens/#:~:text=Cold%20site%20%E2%80%93%20Would%20cost%20$50%2C000,systems%20in%20approximately%20an%20hour.

	T1	**T3**	**T4**	**T5**
V1 on assets A1, A2 and A3	55%	65%	50%	60%
V3 on assets A1, A2, A3, A11	40%	35%	30%	45%
V4 on assets A1, A2, A3, A11	**35%**	**30%**	**45%**	**35%**
V11 on assets A1, A2, A3, A11	40%	50%	35%	30%

Threat/Vulnerability Pairs																
Assets	**T1* V1**	**T1* V3**	**T1* V4**	**T1* V11**	**T3* V1**	**T3* V3**	**T3* V4**	**T3* V11**	**T4* V1**	**T4* V3**	**T4* V4**	**T4* V11**	**T5* V1**	**T5* V3**	**T5* V4**	**T5* V11**
A1	55	40	35	40	65	35	30	50	50	30	45	35	60	45	35	30
A2	55	40	35	40	65	35	30	50	50	30	45	35	60	45	35	30
A3	55	40	35	40	65	35	30	50	50	30	45	35	60	45	35	30
A11	0	40	35	40	0	35	30	50	0	30	45	35	0	45	35	30

Threat/Vulnerability Pairs															
Assets	**T1* V1**	**T1* V3**	**T1* V4**	**T1* V11**	**T3* V1**	**T3* V3**	**T3* V4**	**T3* V11**	**T4* V1**	**T4* V3**	**T4* V4**	**T4* V11**	**T5* V1**	**T5* V3**	**T5* V4**	**T5* V11**
A1	**46.75**	**34**	**29.75**	**34**	**55.25**	**29.75**	**25.5**	**42.5**	**42.5**	**25.5**	**38.25**	**29.75**	**51**	**38.25**	**29.75**	**25.5**
A2	55	40	35	40	65	35	30	50	50	30	45	35	60	45	35	30
A3	55	40	35	40	65	35	30	50	50	30	45	35	60	45	35	30
A11	0	40	35	40	0	35	30	50	0	30	45	35	0	45	35	30

Residual Asset Security Risk:

Risk of Assets A1:
800000* (230%+150%+145%+155%)* **0.85**/100% = $4,624,000 or $4.62M

Risk of Assets A2:
600000 * (230%+150%+145%+155%)/100% = $4,080,000 or $4.08M

Risk of Assets A3:
400000 * (230%+150%+145%+155%)/100% = $2,720,000 or $2.72M

Risk of Assets A11:
500000* (150%+145%+155%)/100% = $2,250,000 or $2.25M

Residual Vulnerability Security Risk:

Risk For V1: [(800000* 230%) * **0.85** + (600000 * 230%) + (400000 * 230%)] / 100 = $4,140,000 or $4.14M
Risk For V3: [(800000* 150%) * **0.85** + (600000 * 150%) + (400000 * 150%) + (500000 * 150%)] / 100 = $3,450,000 or $3.45M
Risk For V4: [(800000 * 145%) * **0.85** + (600000 * 145%) + (400000 * 145%) + (500000 * 145%)] / 100 = $3,335,000 or $3.33M
Risk For V11: [(800000 * 155%)* **0.85** + (600000 * 155%) + (400000 * 155%) + (500000 * 155%)] / 100 = $3,565,000 or $3.56M

Ranking of Security Asset Residual Risks:

Asset	Residual Security Risk	Ranking
A1	$4.62M	1
A2	$4.08M	2
A3	$2.72M	3
A11	$2.25M	4

Ranking of Vulnerability Security Risks:

Asset	Residual Security Risk	Ranking
V1	$4.14M	1
V3	$3.45M	3
V4	$3.33M	4

V11	$3.56M	2

(XIII) Optimized Security Risk Mixed Strategy

Create a list of the Optimal sequence of proposed prevention and response security controls to minimize Security Risk and a list of the Optimal sequence of proposed prevention and response controls to maximize ROI. Estimate a Mixed Strategy budget to minimize Asset Risk. Estimate a Mixed Strategy budget to maximize ROI.

Proposed Controls in an optimized sequence to minimize Residual Security Risk:

- **2-Factor Authentication**
- **VPN**
- **DMZ**
- **Redundant Server**
- **Mirror Site**
- **New CISO Recommendations**
- **Missing MOT Controls**

Optimal sequence to maximize ROI:

- **2-Factor Authentication**
- **VPN**
- **New CISO Recommendations**
- **Missing MOT Controls**
- **DMZ**
- **Redundant Server**
- **Mirror Site**

Security Control Budget: $800000

	T1	T3	T4	T5
V1 on assets A1, A2 and A3	**35%**	**30%**	**20%**	**25%**
V3 on assets A1, A2, A3, A11	50%	55%	65%	65%
V4 on assets A1, A2, A3, A11	45%	40%	55%	45%
V11 on assets A1, A2, A3, A11	40%	50%	35%	30%

Residual Asset Security Risk:

Risk of Assets A1:
800000% * (**110%**+235%+185%+155%)/100% = $5,480,000 or $5.48M

Risk of Assets A2:
600000 * (**110%**+235%+185%+155%)/100% = $4,110,000 or $4.11M

Risk of Assets A3:
400000* (**110%**+235%+185%+155%)/100% = $2,740,000 or $2.74M

Risk of Assets A11:

500000 * (235%+185%+155%)/100% = $2,875,000 or $2.88M

Residual Vulnerability Security Risk:

Risk For V1: [(800000 * 110%) + (600000 * 110%) + (400000 * 110%)] / 100 = $1,980,000 or $1.98M
Risk For V3: [(800000 * 235%) + (600000 * 235%) + (400000 * 235%) + (500000 * 235%)] / 100 = $5,405,000 or $5.41M
Risk For V4: [(800000 * 185%) + (600000 * 185%) + (400000 * 185%) + (500000 * 185%)] / 100 = $4,255,000 or $4.25M
Risk For V11: [(800000 * 155%) + (600000 * 155%) + (400000 * 155%) + (500000 * 155%)] / 100 = $3,565,000 or $3.56M

Ranking of Security Asset Residual Risks:

Asset	Residual Security Risk	Ranking
A1	$5.48M	1
A2	$4.11M	2
A3	$2.74M	4
A11	$2.88M	3

Ranking of Vulnerability Security Risks:

Asset	Residual Security Risk	Ranking
V1	$1.98M	4
V3	$5.41M	1
V4	$4.25M	2
V11	$3.56M	3

Base on the above tables show,V3 has the most residual security risk.

Total Residual Assets Security Risk: $15,205,000 or $15.21M

Vulnerability	Risk Prevention Budget	Risk Response Budget	Mixed Strategy Budget
V1: Clear-text Password Transmission User passwords broadcast unencrypted over LAN during authentication, easily captured by network sniffing tools or malicious software.	$30000	50000	80000
V3: Inadequate Physical Security Compliance Widespread non-compliance with document storage policies, unlocked computers containing sensitive data, and poor after-hours security practices.	$10000	20000	30000

V4: Email System File Access Vulnerability Email utility allows users to attach any accessible file to outgoing messages, enabling data exfiltration via Internet or dial-up connections.	$30000	50000	40000
V11: Untested Contingency Plans Alternative site processing capabilities never verified despite annual testing requirements, may prove illusory during emergencies.	$40000	60000	45000
Total:	$101000	$180000	$195000

(XIV)Conclusion: Risk Reduction and ROI Analysis.

Did the HGA Team Address All Security Risks Based on My Risk Assessment for HGA?

- No. The HGA team's risk mitigation efforts, as outlined in the assessment, partially address the identified security risks but fall short of comprehensive coverage. Key threats such as payroll fraud (T1), operational interruptions (T3), information disclosure (T4), and network threats (T5) are linked to vulnerabilities including clear-text password transmission (V1), physical security non-compliance (V3), email vulnerabilities (V4), and untested contingency plans (V11), affecting critical assets valued at $2.3 million total. Proposed controls like new CISO recommendations, missing MOT controls, 2FA, VPN, DMZ, redundant servers, and mirror sites reduce exploitation probabilities, e.g., V1 from 85% to around 110% adjusted risk factor, but residual risks persist at $15.21 million, representing only a 34% overall reduction from the initial $22.96 million. This indicates gaps in fully mitigating high-probability exploits, particularly V3 at 90%, which remains the dominant residual vulnerability due to ongoing policy violations and incomplete physical safeguards.
- Furthermore, the assessment highlights incomplete alignment with frameworks like NIST 800-53 and FISMA, as current and proposed controls cover some MOT elements but miss others, leaving no vulnerability fully eliminated. For instance, untested contingency plans (V11) retain 60-80% probabilities, enabling extended outages, while physical access issues allow insider and external threats across all assets. Achieving full addressing would require residual risks near zero through exhaustive controls, which the mixed strategy does not deliver, underscoring the need for additional measures like enhanced physical audits and verified recovery testing to protect sensitive payroll data and maintain operational integrity.

Does the Residual Risk Reduction Exceed the Budget for Proposed Controls?

- Yes. The optimized mixed strategy for HGA demonstrates strong cost-effectiveness, with the $800,000 budget yielding a $7.75 million reduction in residual risk, calculated from an initial $22.96 million exposure to $15.21 million post-implementation. This exceeds the investment by over ninefold, achieving an ROI of approximately 869%, driven by sequenced controls such as 2FA and VPN for prevention, alongside redundant servers and mirror sites for response. Prevention-focused elements alone reduce risks like V1 by 35%, while response measures bolster resilience against interruptions, ensuring the financial outlay, covering tools like Nord Layer VPN at $8/user/month and hot site mirroring at $300,000 annually, delivers disproportionate value in safeguarding $3.04 million in assets against high-impact threats.

- In comparison, standalone strategies show even higher ROI potential: prevention at 1,352% ($7.55 million reduction for $520,000) and response at 1,239% ($9.29 million for $750,000), but the mixed approach balances minimization of asset risks (e.g., A1 at $5.48 million residual) with practical implementation. This surplus reduction validates the budget's efficiency, as it not only offsets costs but also mitigates broader consequences like reputational damage (A11) and compliance violations under FISMA and GDPR, positioning HGA for sustained fiscal and operational security without proportional expenditure escalation.

What is the (expected overall security risk reduction Benefit) / (proposed overall security risk budget Cost) ROI ratios for each of the 4 budgets in XIII?

Reduction = Initial Risk Impact – Risk after Implementing strategy

We will be using the Reduction formulate to compare reduction for Prevention, Response and Mixed Strategy.

Asset 1 - Payroll System & Financial Resources

- Initial Risk Impact: $6,440,000 or $6.44M
- Prevention Residual Risk: $5,760,000 or $5.76M
- Response Residual Risk: $4,624,000 or $4.62M
- Mixed Residual Risk: $5,480,000 or $5.48M

Prevention = $6,440,000 - $5,760,000 = $680,000

Response = $6,440,000 - $4,624,000 = $1,816,000

Mixed =$6,440,000 - $5,480,000 = $960,000

Asset 2 - Employee Master Database

- Initial Risk Impact: $4,830,000 or $4.83M
- Prevention Residual Risk: $4,320,000 or $4.32M
- Response Residual Risk: $4,080,000 or $4.08M
- Mixed Residual Risk: = $4,110,000 or $4.11M

Prevention = $4,830,000 - $4,320,000 = $510,000

Response = $4,830,000 - $4,080,000 = $750,000

Mixed =$4,830,000 - $4,110,000 = $720,000

Asset 3 - Time and Attendance Application

- Initial Risk Impact: $3,220,000 or $3.22M
- Prevention Residual Risk: $2,880,000 or $2.88M
- Response Residual Risk: $2,720,000 or $2.72M
- Mixed Residual Risk: $2,740,000 or $2.74M

Prevention = $3,220,000 - $2,880,000 = $340,000

Response = $3,220,000 - $2,720,000 = $500,00

Mixed =$3,220,000 - $2,740,000 = $480,000

Asset 11 - HGA Reputation & Public Trust

- Initial Risk Impact: $2,875,000 or $2.88M
- Prevention Residual Risk: $2,450,000 or $2.45M
- Response Residual Risk: $2,250,000 or $2.25M
- Mixed Residual Risk: $2,875,000 or $2.88M

Prevention = $2,875,000 - $2,450,000 = $430,000

Response = $2,875,000 - $2,250,000 = $630,000

Mixed = $2,875,000 - $2,875,000 = $0

THUS,

- **Total Reduction for Prevention Strategy:**
  $680,000 + $510,000 + 340,000 +$430,000 = $1,960,000 or $1.96M

- **Total Reduction for Response Strategy:**
  $1,816,000 + $750,000 + $500,00 + $630,000 = $3,696,000 or $3.70M

- **Total Reduction for Mixed Strategy:**

  $960,000 + $720,000 + $480,000 +$0 = $2,160,000 or $2.16M

AND,

ROI Calculation Formula = (Risk Reduction Benefit) / (Budget Cost) × 100%

ROI ratio = (Risk Reduction – Budget) / Budget

Prevention Strategy ROI

- Risk Reduction: $1,960,000
- Budget: $520,000
- ROI = ($1,960,000 / $520,000) × 100% = 376.92%
- ROI ratio = 2.77

Response Strategy ROI

- Risk Reduction: $3,696,000
- Budget: $750,000
- ROI = ($3,696,000 / $750,000) × 100% = 492.8%
- ROI ratio =3.93

Mixed Strategy ROI

- Risk Reduction: $2,160,000
- Budget: $800,000
- ROI = ($2,160,000 / $800,000) × 100% = 270%
- ROI ratio =1.7

Strategy	Budget	Risk Reduction	ROI	Ranking
Response	$750,000	$3,696,000	492.8%	1

Prevention	$520,000	$1,960,000	376.92%	2
Mixed	$800,000	$2,160,000	270%	3

Do you recommend a Risk Prevention Strategy or a Risk Response Strategy or a combination such as a Risk reduction strategy or Risk ROI maximization Mixed Strategy? (Conclusion)

- I would recommend the Risk Response Strategy. Because based on the ROI analysis for HGA's proposed security strategies shows that the Risk Response Strategy provides the highest return at 492.8%, saving $3.70 million in risk reduction with a $750,000 investment by implementing controls like redundant servers and mirror sites that mainly address operational interruption vulnerabilities. The Prevention Strategy ranks second with a 376.92% ROI, lowering risk by $1.96 million for $520,000 through measures such as two-factor authentication, VPN, and DMZ controls targeting authentication and network vulnerabilities. The Mixed Strategy, despite having the largest budget of $800,000, results in the lowest ROI at 270%, reducing risk by $2.16 million, and notably fails to reduce the risk for Asset 11 (HGA Reputation & Public Trust) at all, indicating that the combined approach may create inefficiencies rather than benefits. The success of the Response Strategy comes from its ability to effectively mitigate high-impact threats across all four critical assets, notably reducing Asset 1 (Payroll System) risk by $1.816 million compared to Prevention's $680,000 reduction. This demonstrates that resilience-focused controls yield greater value per dollar spent than prevention-only or hybrid approaches, especially given HGA's specific threat landscape.

Part B- Security Risk Management Implementation Plan for BrightSmile Dental Group (Fictional)

Organization: BrightSmile Dental Group (Fictional)

Entity: Sole Proprietorship, Small Private dental company

Department: BrightSmile Dental Group is a fictional small-to-medium healthcare organization representing a private dental practice used for security risk management analysis.

The organization operates as a sole proprietorship with approximately 50 employees, including dentists, hygienists, administrative staff, and IT support personnel.

The practice delivers comprehensive dental services, including general dentistry, cosmetic procedures, orthodontics, oral surgery, and pediatric care.

BrightSmile Dental Group relies on several critical information systems to support daily operations, including:

- Electronic Health Records (EHR)
- Digital imaging systems (X-ray, PACS)
- Practice management and scheduling software
- Billing and insurance processing systems
- Internal email and patient portal platforms

List company critical assets, missing controls, vulnerabilities, potential threats, and security risks for:

1. Access Control Security Risk Management Implementation Controls and Policies:

- Identification Credentials
- Personal Authentication
- Authorization
- Logical Access Control Methods
- Physical Access Control Methods
- Biometric Systems

1. Identification Credentials:

- **Employee ID Number**: A unique numerical identifier assigned to each employee that tracks their identity across all company systems, payroll, and access records.
- **Username/User ID**: A unique alphanumeric identifier that employees use to log into corporate systems, typically following a standard naming format.
- **Email Address**: The corporate email address that serves as both a communication tool and unique identifier for accessing cloud applications.
- **Corporate Badge/ID Card**: A physical identification card displaying employee information, often containing embedded RFID or smart chips for access control.
- **Digital Certificates**: Cryptographic credentials that uniquely identify users and devices for secure network communications, email encryption, and VPN access.
- **API Keys/Access Tokens**: Unique alphanumeric strings assigned to applications or services that identify and authenticate automated systems when accessing company resources.
- **Social Security Number (SSN)**: Government-issued identification number used primarily for payroll, tax reporting, and benefits administration with restricted access.
- **Professional License Numbers**: State or industry-issued certification numbers that verify employee credentials and may be required for specialized system access.
- **Domain Account Credentials**: Active Directory or LDAP account identifiers that uniquely identify users within the company's network infrastructure.
- **Vendor/Contractor ID**: Temporary identification credentials issued to external partners to distinguish them from permanent employees and apply appropriate restrictions.

2. Personal Authentication:

- **Password Authentication**: Employees enter secret alphanumeric passphrases meeting company complexity requirements to verify their identity when accessing systems.
- **Multi-Factor Authentication (MFA)**: Security process requiring two or more verification factors typically password plus mobile code to strengthen authentication security.
- **Single Sign-On (SSO)**: Authentication system allowing employees to log in once and automatically access all connected business applications without re-entering passwords.
- **Biometric Authentication**: Identity verification using unique biological characteristics like fingerprints or facial recognition to provide secure, password-free access.
- **Smart Card/Badge Authentication**: Employees insert or tap their company badge containing an embedded chip, often combined with PIN entry, to authenticate access.
- **Mobile Push Notifications**: Real-time authentication requests sent to employees' registered smartphones where they approve or deny login attempts with a tap.
- **Time-Based One-Time Passwords (TOTP)**: Authenticator apps generate temporary 6-digit codes that refresh every 30 seconds for enhanced authentication security.
- **PIN (Personal Identification Number)**: Short numeric codes that employees enter for quick authentication when unlocking workstations or accessing secure systems.

- **Security Questions**: Pre-configured personal questions used as backup authentication for password resets or account recovery processes.
- **Risk-Based/Adaptive Authentication**: Intelligent system that adjusts authentication requirements based on contextual risk factors like location, device, and time of day.
- **Privileged Access Management (PAM)**: Specialized authentication for IT administrators accessing secure vaults that provide temporary elevated credentials with enhanced monitoring.

3. Authorization:

- **Role-Based Access Control (RBAC):** Assigns permissions based on job roles (admin, user, manager)
- **Attribute-Based Access Control (ABAC):** Grants access based on user attributes, resource properties, and environmental conditions
- **Mandatory Access Control (MAC):** System enforces access based on security classifications and clearance levels
- **Discretionary Access Control (DAC):** Resource owners decide who can access their files and data
- **Least Privilege Principle:** Users receive minimum permissions necessary to perform their job functions
- **Access Control Lists (ACLs):** Detailed lists specifying which users/groups can access specific resources

4. Logical Access Control Methods:

- **Password Authentication**: Username and password combinations to access systems
- **Multi-Factor Authentication (MFA)**: Requires multiple verification factors for login
- **Single Sign-On (SSO)**: One authentication grants access to multiple applications
- **Encryption**: Protects data from unauthorized access using cryptographic algorithms
- **Virtual Private Networks (VPNs)**: Secure encrypted tunnels for remote access
- **Firewalls**: Block unauthorized network traffic based on security rules
- **Access Control Lists (ACLs)**: Define who can read, write, or execute files
- **Session Timeouts**: Automatic logout after periods of inactivity
- **Account Lockout Policies**: Disable accounts after failed login attempts

5. Physical Access Control Methods:

- **Key Cards/Proximity Cards**: Electronic badges that grant entry when scanned
- **Smart Cards with PIN**: Card reader plus PIN entry for two-factor physical access
- **Security Guards**: Personnel monitoring and controlling entry points
- **Locks and Keys**: Traditional mechanical locks for doors and cabinets
- **Mantrap/Airlock Doors**: Two-door systems preventing tailgating
- **Turnstiles and Gates**: Physical barriers requiring authentication to pass
- **Bollards and Barriers**: Vehicle barriers preventing unauthorized vehicle access
- **CCTV/Surveillance Cameras**: Monitor and record activity in restricted areas
- **Motion Detectors**: Alert security when movement detected in unauthorized areas
- **Visitor Management Systems**: Register, badge, and track non-employee access
- **Alarm Systems**: Detect and alert unauthorized entry attempts

6. Biometric Systems:

- **fingerprint Scanners**: Read unique ridge patterns on fingertips
- **Facial Recognition**: Analyze facial features and geometry for identification
- **Iris Scanning**: Capture unique patterns in the colored ring around the pupil

- **Retinal Scanning**: Map blood vessel patterns in the back of the eye
- **Voice Recognition**: Identify individuals by vocal characteristics and patterns

2. Network Infrastructure Security Risk Management Implementation Controls and Policies

- Enclave Protection
- Firewalls Risk Management
- Routers Risk Management

1. Enclave protection:

- **Network Segmentation:** Logically and physically separating critical assets from the rest of the network (e.g., using VLANs or separate subnets) to contain breaches.
- **Access Control Lists (ACLs):** Restricting network traffic flow between segments, ensuring only necessary communication paths are open. This follows the Principle of Least Privilege.
- **Intrusion Detection/Prevention Systems (IDPS):** Deploying sensors to monitor traffic within the enclave for malicious activity and automatically blocking known threats.
- Server Hardening: Applying rigorous security configurations to all systems within the enclave, including disabling unnecessary services, regular patching, and strong password policies.
- **Data Encryption:** Ensuring data at rest (on servers) and data in transit (between enclave systems) is encrypted to protect its confidentiality.
- **Micro-segmentation:** Advanced segmentation that secures individual workloads (e.g., VMs, containers) and controls traffic within the enclave itself.
- **Zero Trust Architecture:** Continuous verification of identity and device compliance should be enforced. Trust is never assumed, even inside the enclave.
- **Least Privilege:** Users and processes should only have the minimum level of access needed. This limits damage if an account or system is compromised.

2. Firewalls Risk Management:

- **Default-Deny Policy:** The foundational rule: Explicitly deny all traffic unless it is expressly permitted by a rule. This is the most secure baseline configuration.
- **Stateful Inspection:** The firewall tracks the state of active connections (e.g., established, listening) to efficiently permit legitimate response traffic while blocking unsolicited traffic.
- **Application Layer Filtering (Next-Gen Firewalls):** Inspecting traffic up to Layer 7 (the application layer) to identify and control specific applications (e.g., blocking Facebook while allowing Office 365).
- **Geographic Filtering:** Blocking traffic originating from or destined for known malicious or unnecessary geographic regions (countries).
- **Centralized Log and Audit:** Sending firewall logs to a SIEM for analysis, correlation, and regular auditing of rule sets to ensure they are optimal and current.
- **Rule Minimization and Review:** Keeping the rule set as small and clear as possible and regularly removing redundant or unused rules to reduce complexity and attack surface.

3. Routers Risk Management:

- **Management Plane Hardening:** Disable unnecessary administrative services (e.g., FTP, HTTP) and ensure secure protocols are used for management access (SSH instead of Telnet, HTTPS instead of HTTP).
- **Strong Authentication and Authorization:** Enforcing strong, unique passwords and Multi-Factor Authentication (MFA) for all administrative accounts. Using Role-Based Access Control (RBAC).

- **Physical Security:** Placing routers in locked, restricted-access areas (e.g., a server room) to prevent unauthorized physical tampering.
- **Interface Access Control Lists (ACLs):** Applying ACLs on inbound and outbound interfaces to filter unwanted traffic, such as Bogon (reserved/private) addresses or specific known malicious sources.
- **Anti-Spoofing Controls:** Ingress and egress filtering should block packets with spoofed IP addresses. This prevents attackers from impersonating trusted systems.
- **Regular Firmware Updates:** Applying the latest security patches and firmware from the vendor immediately to address known vulnerabilities (patch management).
- **Broadcast Suppression:** Configuring the router to limit or suppress broadcast traffic to mitigate potential Denial of Service (DoS) attacks based on broadcast storms.
- **Network Address Translation (NAT):** NAT hides internal IP addresses from external exposure. This adds a layer of obscurity and reduces attack surface.
- **Logging & Monitoring:** Routers should send logs to a SIEM and use SNMPv3 for monitoring. This helps detect unusual traffic or misconfigurations.

3. Network Infrastructure Management Security Risk Management Implementation Controls and Policies

- Ports, Protocols, and Services (PPS) Risk Management
- Device Risk Management
- Device Monitoring, Network Management Risk Management
- Network Authentication, Authorization, and Accounting Risk Management
- Network Intrusion Detection Risk Management
- Switches and VLANs Risk Management
- Virtual Private Network Risk Management

1. **Ports, Protocols and Services(PPS) Risk Management:**

- **Three-Level Port Classification System:** Risk-based framework for managing network ports at the enclave perimeter with Red (deny all), Yellow (conditional with DAA approval), and Green (allow with standard controls) classifications.
- **Block ICMP Echo Request/Reply:** Prevent attackers from using ping commands to map network topology and identify active hosts; also prevents ICMP flood denial-of-service attacks by blocking reconnaissance traffic at the perimeter.
- **Default Deny Policy:** Block all ports by default unless explicitly permitted; classify ports as red (default deny), yellow (conditional allow), or green (best practice) based on operational risk, minimizing information security exposure.
- **Use Encrypted Protocols Only:** Replace insecure protocols: SSH instead of Telnet, HTTPS instead of HTTP, SFTP instead of FTP, SNMPv3 instead of SNMPv1/v2 to protect credentials and data in transit from eavesdropping.
- **IPV4 & IPV6 Address filtering:** Implement Access Control Lists (ACLs) to permit or deny traffic based on source and destination IP addresses for both IPv4 and IPv6 protocols; restrict access to critical services from authorized IP ranges only.

2. **Device Risk Management:**

- **Vulnerability Management System (VMS):** Deploy centralized system interfacing with DoD Enterprise tools to identify security vulnerabilities, track issues through lifecycle from discovery to remediation, and ensure timely patching of critical flaws.

- **Prohibit Telnet for Management:** Never use Telnet for device management as credentials and commands transmit in clear text, making them vulnerable to network sniffing attacks that expose administrative passwords.
- **SSH Version 2 Implementation:** Require SSH v2 with TCP transport for all remote device management; provides encrypted authentication, command execution, and file transfer capabilities using FIPS 140-2 approved algorithms.
- **Out-of-Band (OOB) Management: Dedicated physical or logical network path separate from production network, providing secure device access independent of production infrastructure.**
- **In-Band Management:** Management access through production network infrastructure; requires strong security controls as management traffic shares network with production traffic and potential attackers.
- **Management Access Control Lists:** Restrict SSH and management protocol access to specific administrator IP addresses from internal network only; block all other sources to prevent unauthorized remote access attempts.

3. **Device Monitoring, Network Management Risk Management :**

- **Centralized Syslog Server:** Deploy dedicated server to collect log messages from all communication devices (switches, routers, firewalls, servers) for centralized review, correlation, reporting, storage, and real-time security analysis.
- **Real-Time Log Parsing:** Parse syslog files in real-time to identify suspicious behavior, security violations, and anomalous activity (failed logins, configuration changes, access violations) requiring immediate incident response.
- **Management VLAN Isolation:** Place syslog server on separate management subnet (VLAN 10) isolated from general access and transient traffic to protect logging infrastructure from attacks and unauthorized access.
- **Source IP Filtering:** Configure syslog server to only accept log packets from known managed devices using firewall rules; prevents log injection and spoofing attacks that could hide malicious activity.
- **Maintain Syslog Availability:** Never disable syslog server as it eliminates critical network infrastructure visibility that security analysts depend on for threat detection and ensures logging available for forensic analysis after compromise.

4. **Network Authentication, Authorization, and Accounting Risk management :**

- **Authentication Implementation:** Identify users prior to granting access to network and network services; verify "who you are" through username/password, certificates, or tokens before allowing entry to network resources.
- **Authorization Controls:** Provide authorization for each service based on per-user account lists and profiles; determine "what you can do" after authentication using role-based access control (RBAC) and least privilege.
- **Accounting/Auditing:** Collect and send security server information including user identities, login/logout times, executed commands, packet counts, and byte counts to centralized syslog; track "what you did" for compliance and forensics.
- **Individual User Accounts:** Establish and maintain individual user accounts with unique passwords for each administrator; eliminate shared group accounts that don't allow proper auditing of who is accessing or changing network infrastructure.
- **Password Encryption Requirements:** Encrypt all router passwords so they cannot be viewed when router configuration is displayed on console or copied to documents; apply encryption policies for credentials in transit, memory, and storage.

- **Two-Factor Authentication (2FA):** Implement authentication requiring two different forms of electronic identification: something known (password) + something possessed (token/smart card/mobile app) to significantly reduce risk of compromised credentials.
- **Local Emergency Account:** Configure only one local user account per device as backup when AAA server, SecurID, or token logon services unavailable; set to lowest authorization level (enable command only) to minimize damage.

5. **Network Intrusion Detection Risk Management (NIDS) :**

- **Deploy Signature-Based NIDS:** Implement intrusion detection using known attack signatures and patterns (malware, exploits, reconnaissance) to identify malicious traffic at network perimeter and alert security team.
- **External NIDS Placement:** Install NIDS in front of premise/border router or between router and service delivery gateway to detect perimeter attacks; monitored by certified Computer Network Defense Service Provider (CNDSP).
- **Stealth/Passive Mode Configuration:** Configure IDS using switch SPAN port in stealth mode where monitoring NIC has no IP address on monitored network; eliminates risk of IDS itself being attacked since it has no routable network presence.
- **Out-of-Band Management Connection:** Connect second NIC to Out-of-Band (OOB) management network for IDS administration and alert reporting; keeps management traffic separate from monitored production traffic.
- **Internal Network Monitoring:** Deploy Enclave NIDS to monitor internal network traffic and provide near real-time alarms for network-based attacks, lateral movement, privilege escalation, and insider threats.
- **JID Suite - Near Real-Time Detection:** Deploy Juniper Intrusion Detection for immediate alerts on ongoing attacks occurring on Ethernet/FDDI based networks; provides four operating modes including retrospective analysis and evidence gathering.

6. **Switches, VLANs Risk Management:**

- **VLAN Technology for Segmentation**: Group users into workgroups sharing same network address space regardless of physical location; organize by department, location, or function (Production, Management, Guest, Medical Devices VLANs).
- **Broadcast Domain Isolation:** Broadcast frames only switched between nodes within same VLAN, not propagated to other VLANs; reduces network congestion and prevents broadcast storms from affecting entire network.
- **MAC Address Filtering:** Block input to access port when MAC address doesn't match statically configured or auto-learned authorized addresses; prevents unauthorized devices from connecting even with physical access.
- **Secured IDF/Cabinet:** Keep all switches and cross-connect hardware in secured Intermediate Distribution Frame or enclosed locked cabinet; prevents attackers from gaining privilege mode access through physical console ports.
- **Disconnect Unused Ports:** Disconnect horizontal wiring at switch port or patch panel when no authorized host connected in work area; eliminates physical connection point that attackers could exploit for network access.
- **SNMP Link-Down Traps:** Send link-down trap to SNMP manager when using permanent or timed shutdown methods; provides centralized alerting for security violations across switch infrastructure.

7. **Virtual Private Network Risk Management (VPN) :**

- **Gateway-to-Gateway VPN (Site-to-Site):**Connect two organizational networks by deploying VPN gateway to each network location; establish encrypted tunnel between gateways for secure site-to-site connectivity (branch offices, data centers, cloud services, partner networks).

- **Host-to-Gateway VPN (Remote Access):** Connect remote hosts (laptops, mobile devices) with organization's network through centralized VPN gateway; permit authorized external users to establish individual encrypted connections for remote work, traveling employees, and telecommuting.
- **Host-to-Host VPN (End-to-End):**Connect individual hosts directly to single target host with point-to-point encrypted tunnel; only VPN model providing complete end-to-end protection for data throughout entire transit path from source to destination host.
- **Strong Encryption Algorithms:** Implement AES-256 or stronger encryption algorithms to protect VPN tunnel confidentiality against cryptographic attacks; use secure protocols like IKEv2/IPsec, OpenVPN, or WireGuard.
- **Multi-Factor Authentication for VPN:** Enforce MFA requiring password plus token/certificate/biometric for VPN access to prevent credential compromise; significantly reduces risk of unauthorized remote access.
- **VPN Connection Monitoring:** Monitor and log all VPN connections including connect/disconnect events, duration, data transferred, and source locations; review logs for anomalies and unauthorized access attempts.
- **VPN Client Compliance Checking:** Verify endpoint security posture before granting VPN access (antivirus updated, patches current, firewall enabled); deny access to non-compliant devices to prevent introducing threats.
- **IPsec VPN:** Internet Protocol Security provides network layer encryption for both site-to-site and remote access VPNs. Works with all IP-based applications; provides strong security; operates transparently to applications.
- **SSL/TLS VPN:** Secure Sockets Layer / Transport Layer Security VPN operates at application layer (Layer 7). No client software installation required; works through firewalls on port 443; granular application-level access control; easier for users.

4. Database Security Risk Management Implementation Controls and Policies

- Authentication – User accounts
- Authorization
- Confidentiality
- Data Integrity
- Auditing
- Replication and Federation
- Clustering
- Backup and Recovery
- OS Protections
- Application protections
- Network protections
- Security Design and Configuration
- Enclave and Computing environment
- Business Continuity
- Vulnerability and Incident management

1. **Authentication – User accounts:**

- **Multi-Factor Authentication (MFA):** MFA requires users to verify their identity using at least two forms of credentials, such as a password and a one-time code to reducing the risk of unauthorized access even if one credential is compromised.
- **Strong Password Policy:** Enforcing password complexity, minimum length, and periodic changes prevents brute-force and dictionary attacks while encouraging secure password habits.

- **Account Lockout Mechanism:** Systems automatically lock an account after a set number of failed login attempts to defend against password-guessing and automated attacks.

2. **Authorization:**
- **Role-Based Access Control (RBAC):**Users are assigned permissions based on their job roles, ensuring they only have access to information necessary for their responsibilities.
- **Principle of Least Privilege:** Every user or system is given the minimum level of access required to perform their functions, minimizing potential damage from insider or compromised accounts.
- **Access Review and Revocation:** Regular reviews ensure that users who change roles or leave the organization no longer retain access to sensitive systems.

3. **Confidentiality:**
- **Data Encryption (in Transit and at Rest):**Encryption technologies like AES and TLS protect sensitive information from interception or unauthorized disclosure during storage and transmission.
- **Data Classification and Labeling:** Classifying data as public, confidential, or restricted helps determine the appropriate level of protection and access control.
- **Secure Communication Channels:** Implementing secure email gateways, VPNs, and HTTPS ensures confidentiality in organizational communications.

4. **Data Integrity:**
- **Hashing Algorithms (e.g., SHA-256):** Hashing verifies that data has not been altered by generating a unique checksum that changes if even a single bit is modified.
- **Digital Signatures:** Digital signatures use cryptographic keys to authenticate the origin and verify the integrity of electronic documents and transactions.
- **Integrity Monitoring Tools:** Continuous monitoring systems alert administrators when unauthorized file modifications occur.

5. **Auditing:**
- **Security Information and Event Management (SIEM):**SIEM tools collect, analyze, and correlate logs from multiple systems to detect and respond to security incidents.
- **Audit Trail Maintenance:** Keeping detailed logs of user activities allows tracking of events for compliance and forensic investigations.
- **Regular Compliance Audits:** Periodic internal or third-party audits ensure adherence to regulations like HIPAA, GDPR, and NIST standards.

6. **Replication and Federation:**
- **Encrypted Data Replication:** Data replicated between servers or sites is encrypted to prevent interception and unauthorized access during transmission.
- **Federated Identity Management:** Systems like SAML or OAuth2 enable secure authentication across multiple domains or organizations without sharing credentials.
- **Redundant Systems:** Maintaining synchronized backups across data centers ensures continuous availability and resilience against data loss.

7. **Clustering:**
- **Failover Clustering:** In the event one server fails, another node automatically takes over, ensuring high availability and minimal service disruption.
- **Secure Node Communication:** Communication between clustered nodes is encrypted and authenticated to prevent unauthorized manipulation.
- **Load Balancing:** Distributing workloads across multiple servers enhances performance and prevents overloading a single system.

8. **Backup and Recovery:**
- **Regular Automated Backups:** Frequent, scheduled backups minimize data loss during system failures or cyber incidents.
- **Encrypted Backup Storage:** Storing backups in encrypted form ensures confidentiality even if backup media is stolen or lost.
- **Disaster Recovery Plan (DRP):** A documented DRP outlines procedures for data restoration and system recovery after a breach or outage.

9. **OS Protections:**
- **Patch Management:** Regularly applying operating system updates closes known vulnerabilities and reduces exploit risks.
- **File System Permissions:** Configuring access controls at the OS level ensures users can only read, modify, or execute files appropriate to their roles.
- **System Hardening:** Disabling unnecessary services and ports minimizes attack surfaces and potential exploitation vectors.

10. **Application Protections:**
- **Input Validation:** Ensuring that applications only accept properly formatted data prevents injection and cross-site scripting attacks.
- **Code Review and Testing:** Regular code audits identify vulnerabilities before deployment, ensuring secure development practices.
- **Web Application Firewall (WAF):** A WAF filters and monitors HTTP traffic to protect applications from common web-based attacks.

11. **Network Protections:**
- **Firewalls:** Firewalls control incoming and outgoing traffic based on predefined rules, preventing unauthorized access to network segments.
- **Network Segmentation:** Dividing the network into isolated zones limits the spread of malware and restricts access to critical assets.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** These systems monitor traffic for suspicious activity and can automatically block malicious behavior.

12. **Security Design and Configuration:**
- **Security Baselines:** Establishing standard configurations ensures systems are deployed with consistent and secure settings.
- **Change Control Procedures:** All system changes are reviewed and approved to prevent accidental introduction of vulnerabilities.
- **Defense in Depth:** Layering multiple security controls creates redundancy, reducing the chance of a single point of failure.

13. **Enclave and Computing Environment:**
- **Network Isolation:** Sensitive computing environments are separated from general networks to contain security risks.
- **Endpoint Protection (EDR/XDR):** Advanced endpoint tools monitor, detect, and respond to malicious activity on user devices.
- **Virtualization Security:** Implementing hypervisor security controls protects virtual machines from escape attacks or compromise.

14. **Business Continuity:**

- **Business Continuity Planning (BCP):** BCP outlines how essential operations continue during crises, ensuring minimal disruption.
- **Redundant Infrastructure:** Backup power supplies, secondary sites, and mirrored systems ensure operational resilience.
- **Crisis Communication Plan:** Establishing communication channels ensures employees and stakeholders receive accurate updates during incidents.

15. Vulnerability and Incident Management:

- **Regular Vulnerability Scanning:** Automated scans identify and prioritize weaknesses in systems and applications for timely remediation.
- **Incident Response Plan (IRP):** A structured plan defines how to detect, contain, and recover from cybersecurity incidents efficiently.
- **Post-Incident Analysis:** Reviewing incidents helps identify root causes and improve future response strategies.

5. Applications Development Security Risk Management Implementation Controls and Policies

- Program Management
- Application Data Handling
- Authentication
- Use of Cryptography
- User Accounts
- Input Validation
- Auditing
- Configuration Management
- Testing
- Deployment

1. Program Management:

- **Applications Development:** Designed, developed, and delivered application solutions by coordinating requirements, managing development cycles, and ensuring alignment with organizational and technical standards.
- **Security Management:** Implemented security frameworks and best practices to safeguard applications and infrastructure, including access control, encryption, and continuous monitoring.
- **Risk Management:** Identified, assessed, and prioritized technical and operational risks, developing mitigation strategies to reduce exposure and enhance overall program resilience.
- **Security Compliance:** Ensured all applications and processes conformed to regulatory requirements, organizational policies, and industry best practices through ongoing audits and compliance reviews.
- **Secure SDLC Oversight:** Integrated security checkpoints, such as code review, threat modeling, and vulnerability scanning, into the software development lifecycle to ensure secure delivery of applications.

2. Application Data Handling:

- **Data Classification:** All application data should be categorized based on sensitivity levels, such as public, internal, confidential, or restricted to ensure each dataset receives proper protection and management throughout its lifecycle.
- **Data Encryption:** Sensitive data must be encrypted both during transmission, using secure protocols like TLS 1.3, and when stored, with strong algorithms such as AES-256, to maintain confidentiality and prevent unauthorized access.
- **Access Control:** Apply least-privilege access principles so that users and applications can only access data necessary for their roles, reducing exposure risks.
- **Data Sanitization:** Set up automated processes for data retention and sanitization that securely delete or anonymize data no longer needed, ensuring compliance with privacy laws like GDPR or HIPAA.
- **Tokenization and Hashing:** Use tokenization or cryptographic hashing to protect personally identifiable information (PII) and other sensitive data, lowering the risk of exposure in case of a breach.

3. **Authentication :**

- **Multi-Factor Authentication (MFA):** Require users to verify their identities using at least two factors, such as a password combined with a one-time code or biometric verification, greatly reducing the risk of unauthorized access.
- **Strong Password Policy:** Enforce rules for complex passwords, including minimum length and character variety, along with regular password changes, to prevent brute-force or dictionary-based attacks.
- **Account Lockout Mechanism:** Automatically lock accounts after a set number of failed login attempts to discourage automated guessing attacks and notify administrators of possible intrusion attempts.
- **Session Timeout:** Set automatic session timeouts and re-authentication requirements after periods of inactivity to safeguard against unauthorized access through unattended systems.
- **Centralized Authentication Management:** Use Single Sign-On (SSO) or LDAP-based systems to securely and consistently manage identities across multiple applications.

4. **Use of Cryptography:**

- **Approved Cryptographic Standards:** Only approved cryptographic algorithms such as AES, RSA, and ECC should be used, while deprecated algorithms like MD5 and SHA-1 must be avoided to maintain strong encryption standards.
- **Key Management:** Encryption keys must be securely stored, rotated periodically, and managed using secure key vaults or hardware security modules (HSMs) to prevent unauthorized key access.
- **Digital Signatures:** Use digital signatures to verify data integrity and authenticity, ensuring that data has not been altered or tampered with during transmission.
- **Certificate Management:** Manage SSL/TLS certificates responsibly by obtaining them from trusted certificate authorities, monitoring their validity, and renewing them before expiration.
- **Encryption Auditing:** Conduct regular reviews of cryptographic implementations to identify weaknesses or outdated configurations, updating them as needed.

5. **User Accounts:**

- **Role-Based Access Control (RBAC):** Assign system permissions strictly based on user roles to restrict administrative privileges and prevent excessive access rights.
- **Account Lifecycle Management:** Implement automated processes for creating and removing accounts to ensure access is granted, changed, or revoked promptly as employment status updates.
- **Least Privilege Principle:** Enforce the principle of least privilege across all accounts, ensuring users only access resources necessary for their job functions.

- **Account Monitoring:** Continuously observe account activities for unusual behavior such as repeated login failures, privilege escalation, or access outside of normal hours.
- **Audit Logging:** Keep detailed logs of account creation, modification, and deletion to support forensic investigations and compliance reporting.

6. **Input Validation:**

- **Comprehensive Input Sanitization:** All user-provided data must be validated, sanitized, and encoded to defend against injection-based attacks such as SQL injection and cross-site scripting (XSS).
- **Whitelist Validation Approach:** Accept only input that matches defined acceptable patterns and formats to minimize the risk of malicious payloads being processed by the application.
- **Server-Side Validation:** Input validation should be enforced on the server side rather than relying solely on client-side mechanisms, ensuring consistency and robustness.
- **Output Encoding:** Properly encode dynamic output content to prevent malicious data from executing as code in a user's browser environment.
- **Error Handling:** Design secure error-handling routines that display generic error messages to users while logging detailed error information internally for debugging and security reviews.

7. **Auditing:**

- **Comprehensive Logging:** Ensure that critical events, including authentication, authorization, configuration changes, and system errors are logged in sufficient detail for post-incident analysis.
- **Centralized Log Management:** Aggregate and store all logs in a centralized Security Information and Event Management (SIEM) system to enable real-time monitoring and alerting.
- **Immutable Log Storage:** Store audit logs in tamper-proof locations to preserve their integrity and usefulness during forensic investigations.
- **Periodic Review:** Regularly review logs to detect unusual patterns, such as failed login attempts, privilege misuse, or data exfiltration activities.
- **Compliance Auditing:** Conduct routine audits to ensure adherence to internal policies and regulatory frameworks such as PCI DSS or NIST 800-53.

8. **Configuration Management:**

- **Baseline Configuration:** Maintain a securely approved baseline configuration for all systems and applications to ensure consistency and reduce security drift.
- **Change Control Process:** All configuration changes must go through formal review and approval processes to prevent unauthorized or risky modifications.
- **Patch and Update Management:** Apply patches and updates promptly to address known vulnerabilities and sustain system stability.
- **Configuration Scanning:** Regularly scan systems using automated tools to identify deviations from security baselines and implement necessary corrections.
- **Documentation and Version Control:** Keep detailed records of configuration changes and enforce version control to enable rollback and ensure traceability.

9. **Testing:**

- **Static Application Security Testing (SAST):** Conduct automated source code analysis to detect security vulnerabilities before compilation or deployment.
- **Dynamic Application Security Testing (DAST):** Perform runtime testing of applications in controlled environments to identify security issues during operation.
- **Penetration Testing:** Carry out regular penetration tests simulating real-world attacks to assess the effectiveness of current security controls.

- **Security Regression Testing:** Reevaluate application security after updates or patches to confirm no new vulnerabilities are introduced.
- **Continuous Integration Testing:** Incorporate security testing into the CI/CD pipeline to ensure automated and consistent security checks throughout development.

10. **Deployment:**

- **Secure Build Pipeline:** Use verified, isolated build environments to ensure that code deployed to production is free from tampering and properly authenticated.
- **Environment Separation:** Maintain strict separation between development, staging, and production environments to prevent unauthorized data access and accidental code leaks.
- **Change Management Approval:** Require formal approval for all production deployments to ensure that releases meet both functional and security requirements.
- **Post-Deployment Monitoring:** Implement monitoring systems that continuously track application performance, detect anomalies, and alert teams to potential security events.
- **Incident Response Readiness:** Ensure that incident response plans are in place and tested so that teams can quickly respond to vulnerabilities discovered after deployment.

6. Wireless Security Risk Management Implementation Controls and Policies

- Wireless LAN Risk Management
- Wireless PAN Risk Management
- Wireless WAN Risk Management
- Wireless RFID Risk Management
- Wireless PED Risk Management

1. **Wireless LAN (WLAN) Risk Management:**

- **WPA3/WPA2-Enterprise with 802.1X Authentication:** This provides strong encryption and centralized user authentication using a RADIUS server. It prevents unauthorized access and protects against credential interception or brute-force attacks.
- **Wireless Intrusion Detection/Prevention Systems (WIDS/WIPS):** WIDS/WIPS continuously monitor the airspace for rogue access points, fake SSIDs, and unusual wireless behavior. When threats are detected, the system alerts administrators or automatically blocks malicious devices.
- **Network Segmentation with VLANs:** Segmenting wireless networks isolates users, devices, and sensitive resources to prevent unnecessary exposure. This limits lateral movement and reduces the blast radius of a compromise.
- **Secure Access Point Configuration:** Changing default credentials, enabling strong admin passwords, and disabling SSID broadcasting reduces the likelihood of unauthorized AP access. Properly configured access points minimize vulnerabilities caused by weak settings.
- **Regular Wireless Vulnerability Scanning:** Routine scanning identifies misconfigurations, outdated encryption settings, and exposed wireless devices. This ensures weaknesses are discovered and remediated before attackers can exploit them.
- **SSID Management (Broadcast and Naming Controls):** SSID management reduces exposure by controlling how the network name is displayed and discovered by nearby devices. Using non-identifying SSID names and disabling SSID broadcast makes it harder for attackers to perform reconnaissance or target the organization’s wireless infrastructure.

2. **Wireless PAN (WPAN) Risk Management:**

- **Secure Bluetooth Pairing Modes**: Methods such as numeric comparison and passkey entry verify both devices and prevent man-in-the-middle attacks. These stronger pairing methods eliminate risks associated with simple or default PINs.
- **Disable Bluetooth Discoverable Mode:** Keeping devices hidden from public scanning reduces exposure to unsolicited pairing attempts. This prevents attackers from identifying your device as a target in crowded environments.
- **Enable PAN-Level Encryption (Bluetooth, ZigBee, NFC):** Encryption ensures that data transmitted between devices cannot be intercepted or manipulated. This protects sensitive information commonly sent through IoT devices, wearables, and mobile accessories.
- **Remove or Disable Unneeded Services/Profiles:** Turning off unused capabilities like file transfer, tethering, or audio streaming eliminates unnecessary attack paths. Fewer active services mean fewer places an attacker can exploit vulnerabilities.
- **Regular Firmware and Security Updates:** Keeping Bluetooth, ZigBee, and NFC firmware updated ensures devices are patched against known vulnerabilities like BlueBorne. Updates also enhance crypto strength and remove insecure legacy features.

3. **Wireless WAN (WWAN) Risk Management:**

- **VPN Encryption for Cellular Traffic:** Using a VPN encrypts all mobile data, preventing interception over cellular networks or by rogue base stations. This protects the confidentiality and integrity of communications, especially outside corporate networks.
- **Mobile Device Management (MDM) Controls:** MDM enforces baseline security settings like encryption, screen-lock policies, and remote wipe capability. It ensures consistent protection for all devices connecting through cellular networks.
- **Disable Hotspots and Tethering:** Unauthorized hotspots create unmonitored wireless entry points that attackers can exploit. Disabling tethering ensures users cannot bypass corporate security controls or leak internal data.
- **Restrict Devices to Approved APNs:** Limiting devices to trusted Access Point Names (APNs) ensures they communicate only with authorized cellular networks. This prevents devices from connecting to malicious carriers or unsecure networks.
- **IMSI Catcher/Stingray Detection Measures:** Monitoring for rogue cellular towers helps defend against attacks that intercept calls, messages, and mobile data. These protections ensure devices do not reveal subscriber identities or connect to unauthorized base stations.

4. **Wireless RFID Risk Management:**

- **RFID Encryption and Mutual Authentication:** Encrypting RFID communications protects tag data from being intercepted or cloned. Mutual authentication ensures that both the reader and the tag are legitimate before exchanges occur.
- **Reduce Reader Antenna Power:** Lowering signal strength reduces how far RFID tags can be read, minimizing exposure to unauthorized individuals. This prevents attackers from performing long-range scanning or skimming.
- **RFID Shielding (Faraday Sleeves, Blockers):** Shielding prevents RFID tags from being read when they are not in active use. This is especially critical for employee badges and payment cards that are susceptible to covert scanning.
- **Harden RFID Readers:** Securing readers with strong passwords, firmware updates, and disabled unused ports reduces the risk they will be tampered with. A compromised reader can be used to rewrite tags or steal sensitive data.
- **Implement Tag Kill or Disable Commands:** Deactivating RFID tags after use prevents them from being misused for tracking or unauthorized re-reads. This is commonly required for supply chain tags once items leave the controlled environment.

5. **Wireless PED (Portable Electronic Device) Risk Management:**

- **Full-Device Encryption:** Encrypting the entire device protects stored data even if the PED is lost or stolen. Without the correct decryption key, attackers cannot access sensitive files or credentials.
- Strong Authentication and Auto-Lock: Using biometrics, PINs, and fast auto-lock settings ensures only authorized users can access the device. This reduces risks when a device is left unattended or misplaced momentarily.
- **Mobile Device Management (MDM) Enforcement:** MDM deploys security policies, controls app installations, and enables remote wipe for compromised or lost devices. It ensures all corporate devices meet consistent security standards.
- Disable Unused Wireless Interfaces (Wi-Fi, Bluetooth, NFC): Turning off unnecessary radios reduces the number of wireless attack vectors available to adversaries. It prevents exploitation of idle interfaces such as BlueBorne or NFC skimming.
- Endpoint Security and App Restrictions: Installing mobile antivirus, EDR tools, and limiting apps to approved sources prevents malware and data leaks. These protections ensure PEDs remain safe even when used across multiple networks.
- **BYOD (Bring Your Own Device) Policy Control:** A BYOD policy establishes security requirements for personally owned devices before they are allowed to connect to organizational wireless networks. It ensures that all personal devices meet minimum standards, such as encryption, strong authentication, approved applications, and MDM enrollment reducing the risk of malware, data leakage, or insecure configurations entering the enterprise environment.

(7) Across all Security Risk areas 1-6 from above provide a table for:

(a)List of Cybersecurity Implementation controls that exist at your company

1. Access Control Security Risk Management Implementation Controls and Policies:

- **Identification Credentials:**
- **Employee ID Number**: Each staff member receives a unique ID number used in the practice management system (Dentrix, Eaglesoft) to track access to patient records, clock in/out for payroll, and maintain audit trails for HIPAA compliance.
- **Username/User ID**: All clinical and administrative staff have unique usernames for logging into EHR systems, practice management software, and insurance portals to ensure individual accountability for accessing Protected Health Information (PHI).
- **Email Address**: Staff corporate email addresses are used for secure patient communication through HIPAA-compliant portals, receiving authentication codes for insurance verification systems, and accessing cloud-based scheduling applications.
- **Professional License Numbers**: BrightSmile Dental Group (Fictional) Dentists and hygienists' state license numbers are stored in the practice management system for insurance credentialing, claim submissions, and regulatory compliance verification.
- **Social Security Number (SSN)**: Collected during employee onboarding and stored securely in HR files for payroll processing, tax reporting (W-2s), and benefits enrollment, with access restricted to office manager only.

- **Personal Authentication:**
- **Password Authentication**: All staff members use unique passwords to access the practice management system, EHR, digital imaging software (X-rays), and insurance portals, with passwords required to meet minimum complexity (8+ characters, mix of letters/numbers).
- **PIN (Personal Identification Number)**: Dentists and hygienists use 4-6 digit PINs for quick authentication when moving between operatories to access patient charts on chairside computers or unlock workstations during treatment.

- **Security Questions**: Used as backup authentication when staff forget passwords; the office manager can verify identity through pre-set questions before resetting credentials.
- **Multi-Factor Authentication (MFA)**: Implemented for remote access to practice management systems and when accessing insurance company portals from home, but not always enforced for in-office workstation access.

- **Authorization:**
- **Role-Based Access Control (RBAC)**: Staff permissions assigned based on job role—dentists have full access to all patient records; hygienists access treatment notes and X-rays; front desk staff access scheduling and billing but limited clinical information; insurance coordinators access billing and insurance modules.
- **Least Privilege Principle**: Implemented through practice management software settings where front desk staff cannot access clinical notes, dental assistants cannot modify billing, and insurance coordinators cannot alter treatment plans.
- **Access Control Lists (ACLs)**: Basic file permissions set on shared network drives where only office manager can access employee files, payroll data, and practice financial reports.
- **Discretionary Access Control (DAC)**: Partially implemented dentists can grant temporary access to specific patient files for consultations or referrals, but full DAC flexibility is limited.

- **Logical Access Control Methods:**
- **Password Authentication**: Primary method for accessing all computer systems, practice management software, and digital imaging systems.
- **Encryption**: Patient data encrypted in transit when transmitting electronic claims to insurance companies and when using email for patient communication through HIPAA-compliant platforms.
- **Session Timeouts**: Workstations automatically lock after 10-15 minutes of inactivity per HIPAA requirements, requiring password re-entry.
- **Account Lockout Policies**: Accounts temporarily locked after 3-5 failed password attempts to prevent brute force attacks.
- **Firewalls**: Network firewall installed on office router to block unauthorized external access to practice management system and patient database.
- **Virtual Private Networks (VPNs)**: Implemented if staff access practice management system remotely from home, creating encrypted tunnel to office network.

- **Physical Access Control Methods:**
- **Locks and Keys**: Traditional deadbolts on office entrance, treatment rooms, supply closets, and medication cabinets to secure controlled substances and valuable equipment.
- **Alarm Systems**: Security alarm system that arms after hours, detecting unauthorized entry through doors and windows, with monitoring service that alerts police.
- **CCTV/Surveillance Cameras**: Security cameras at entrance, reception area, and parking lot to monitor activity, deter theft, and provide evidence if incidents occur.
- **Visitor Management**: Front desk staff register visiting patients, pharmaceutical reps, and equipment technicians; visitors must check in and are escorted in clinical areas.
- **Motion Detectors**: We have implemented this in our employee parking lot to ensure there's not an unauthorize people park the car in our parking lot.

2. Network Infrastructure Security Risk Management Implementation Controls and Policies

- **Enclave Protection:**
- **Network Segmentation via VLANs:** BrightSmile Dental Group (Fictional) has logically segmented its internal network into multiple Virtual LANs (VLANs). This architecture isolates

traffic for Clinical systems, Staff workstations, Patient Wi-Fi, and IoT devices to contain potential threats.

- **Secure Wireless Architecture:** BrightSmile Dental Group (Fictional) operates distinct, segregated wireless networks. A secure " BrightSmile Dental Group (Fictional)_Staff" network is used for business operations, while an isolated " BrightSmile Dental Group (Fictional)_Guest" network is provided for patients and visitors.
- **Endpoint Detection and Response (EDR):** BrightSmile Dental Group (Fictional) protects all company-owned workstations and servers with a centralized Endpoint Detection and Response (EDR) solution, which provides advanced threat prevention and detection capabilities.
- **Full Disk Encryption (FDE):** BrightSmile Dental Group (Fictional) has enabled full disk encryption on all practice-owned laptops and mobile devices to protect data at rest in the event of loss or theft.
- **Mobile Device Management Policy:** BrightSmile Dental Group (Fictional) has implemented a Mobile Device Management (MDM) policy that governs the security requirements for all mobile devices accessing practice data, including encryption, remote wipe capabilities, and approved applications.
- **Mandatory Security Awareness Training:** BrightSmile Dental Group (Fictional) requires all employees to complete initial and annual cybersecurity training. This program includes training on identifying phishing, social engineering, and proper password hygiene, reinforced by periodic simulated phishing exercises.
- **Role-Based Access Control (RBAC) Policy:** BrightSmile Dental Group (Fictional) enforces a strict access control policy based on job function. This ensures staff can only access the patient data and software systems necessary for their specific roles, adhering to the principle of least privilege.
- **Password & Multi-Factor Authentication (MFA) Policy:** BrightSmile Dental Group (Fictional) enforces a policy requiring strong, unique passwords for all systems. Furthermore, Multi-Factor Authentication (MFA) is mandatory for all cloud-based services, including practice management software and email.

- **Firewalls Risk Management:**
- **Next-Generation Firewall (NGFW):** BrightSmile Dental Group (Fictional) utilizes a business-grade Unified Threat Management (UTM) firewall at the network perimeter. This provides stateful inspection, intrusion prevention (IPS), and web content filtering.
- **Web Filtering and Content Control:** BrightSmile Dental Group (Fictional) implements web filtering technology to block access to malicious and inappropriate websites from our business networks, reducing the risk of malware infections.
- **Documented Incident Response & Data Backup Plans:** BrightSmile Dental Group (Fictional) has a formal Incident Response Plan to guide actions during a security breach. BrightSmile Dental Group (Fictional) also maintains a robust Data Backup Policy, ensuring critical data is backed up regularly using a secure 3-2-1 strategy and tested quarterly.

- **Routers Risk Management:**
- **Email Security Filtering:** BrightSmile Dental Group (Fictional) utilizes advanced threat protection and spam filtering on our email platform to block malicious attachments, links, and phishing attempts before they reach user inboxes.
- **Automated Patch Management System:** BrightSmile Dental Group (Fictional) employs an automated patch management system that ensures all operating systems and applications are kept current with the latest security updates on a regular schedule.
- **VPN with Multi-Factor Authentication:** BrightSmile Dental Group (Fictional) provides a secure Virtual Private Network (VPN) protected with multi-factor authentication for authorized remote access to our internal network systems.

- **Controlled Physical Access:** BrightSmile Dental Group (Fictional) secures server and network infrastructure in a locked closet. BrightSmile Dental Group (Fictional) also requires the use of cable locks for all company-owned laptops and mobile devices when left unattended.
- Workstation Auto-Lock Policy: BrightSmile Dental Group (Fictional) has configured all computers and workstations with automatic screen locks that activate after a maximum of 10 minutes of inactivity, requiring a password to resume.
- **Secure Media Destruction Procedures:** BrightSmile Dental Group (Fictional) implements secure destruction procedures for all media containing PHI, including paper records and digital storage devices, using cross-cut shredders and certified data destruction services.
- **Visitor Access Management:** BrightSmile Dental Group (Fictional) maintains a visitor log and requires all non-staff members to be escorted while in clinical and administrative areas. All visitors are restricted to the guest Wi-Fi network.

3. Network Infrastructure Management Security Risk Management Implementation Controls and Policies

- **Ports, Protocols, and Services (PPS) Controls:**
- **Three-Level Port Classification System:** BrightSmile Dental Group (Fictional) uses a Red/Yellow/Green system to manage network ports. Red ports (Telnet, FTP, SMB v1) are always blocked due to high security risk. Yellow ports (HTTP, RDP, SNMP) require management approval before use. Green ports (HTTPS, SSH, DNS) are allowed as secure best practices. This is enforced on all firewalls and network devices.
- **Default Deny Firewall Policy:** BrightSmile Dental Group (Fictional) blocks all incoming traffic from the internet is blocked unless specifically approved. Only VPN connections and HTTPS for cloud services are permitted inbound. This prevents attackers from accessing internal systems.
- **ICMP Protocol Restrictions:** BrightSmile Dental Group (Fictional) blocks ICMP Echo (ping) is blocked at the network edge to prevent attackers from mapping the network. ICMP Redirect is disabled to prevent routing attacks. Traceroute is blocked to hide internal network structure. Internal ICMP is allowed for troubleshooting.
- **IPv4 & IPv6 Address Filtering:** BrightSmile Dental Group (Fictional) blocks private IP addresses are blocked from entering via the internet to prevent spoofing. SSH access is restricted to the management workstation only. Geographic filtering blocks connections from non-US countries except Canada for business needs.
- **Encrypted Protocol Enforcement:** BrightSmile Dental Group (Fictional) require all network management uses encryption. SSH v2 replaces Telnet. HTTPS replaces HTTP. SFTP replaces FTP. SNMPv3 replaces older insecure versions. All encryption meets FIPS 140-2 federal standards.

- **Device Management Controls:**
- **Vulnerability Management System (VMS):** BrightSmile Dental Group (Fictional) runs tenable Nessus scanner runs weekly on network devices, monthly on servers/workstations. Critical vulnerabilities are fixed within 7 days, High within 30 days, Medium within 90 days. All findings are tracked until resolved.
- **Patch Management Program:** BrightSmile Dental Group (Fictional) updates workstations update automatically during lunch hours. Servers are patched monthly on Saturday nights during maintenance windows. Network devices are updated quarterly. All patches are tested before deployment and backups are taken before changes.
- **Out-of-Band Management Network (VLAN 10):** BrightSmile Dental Group (Fictional) operates a separate isolated network is used only for managing network equipment. This network has no connection to regular office systems. Only one hardened administrator workstation can access it. Management remains available even if the main network is compromised.

- **SSH Protocol Implementation:** BrightSmile Dental Group (Fictional) manage all network devices are managed via encrypted SSH v2 protocol only. Telnet is completely disabled. 2048-bit encryption keys are required. Sessions timeout after 10 minutes of inactivity with maximum 3 login attempts.
- **Management Access Control Lists:** BrightSmile Dental Group (Fictional) limit SSH access to network devices is limited to a single IP address - the administrator's workstation. All other connection attempts are blocked and logged. This prevents unauthorized management even if someone gains network access.

- **Device Monitoring Controls:**
- **Centralized Syslog Server:** BrightSmile Dental Group (Fictional) operates a central log server that receives logs from all network devices, servers, and security systems. Logs include login attempts, configuration changes, security violations, and system errors. Active logs are kept 90 days; archived logs retained 7 years for HIPAA compliance.
- **Real-Time Log Parsing and Alerting:** BrightSmile Dental Group (Fictional) uses an automated system that watches logs continuously for security threats. Critical events like multiple failed logins, unauthorized changes, or malware detections trigger immediate SMS and email alerts to IT Administrator. Daily summaries report less urgent warnings.
- **Syslog Server Security Hardening:** BrightSmile Dental Group (Fictional) places the log server on the isolated management network. Firewall rules only accept logs from known devices. Only the management workstation can access it. Logs are stored in tamper-proof format preventing attackers from deleting evidence.
- **Security Monitoring Dashboard:** BrightSmile Dental Group (Fictional) maintains a real-time web dashboard showing current security status including failed logins, blocked traffic, device status, recent changes, active VPN users, and bandwidth usage. Updates every 60 seconds. Accessible from management workstation only.
- **SPAN Port Configuration for Traffic Mirroring:** BrightSmile Dental Group (Fictional) configures the core switch to copy all network traffic to a monitoring port where the intrusion detection system connects. This allows security monitoring of all communications without disrupting normal operations.

- **Network Authentication, Authorization, and Accounting (AAA) Controls:**
- **Active Directory Domain Services:** BrightSmile Dental Group (Fictional) operates a central Windows server that manages all user accounts and passwords. 15 staff members have individual accounts organized by role (Dentists, Hygienists, Administrative, IT). Password policy requires 12+ characters with complexity, 90-day expiration, and account lockout after 5 failed attempts.
- **RADIUS Server for Network Access:** BrightSmile Dental Group (Fictional) uses a separate authentication server (192.168.50.70) that validates WiFi connections, VPN access, and network device logins. Integrates with Active Directory to use the same credentials everywhere. All authentication attempts are logged for security review.
- **Multi-Factor Authentication (MFA) Policy:** BrightSmile Dental Group (Fictional) requires VPN, network device management, management workstation login, and email to need password PLUS a second factor (mobile app code, hardware token, or push notification). All staff must enroll within 7 days. Prevents access even if password is stolen.
- **Individual User Accounts:** BrightSmile Dental Group (Fictional) assigns each staff member their own unique account - no shared passwords. Accounts follow naming standard (first initial + last name). Terminated employee accounts are immediately disabled. This creates complete audit trail showing exactly who did what.
- **Role-Based Access Control (RBAC):** BrightSmile Dental Group (Fictional) assigns access based on job function. Dentists get full patient record access. Hygienists get limited access to assigned

patients only. Administrative staff access billing and scheduling but not clinical notes. IT staff have system access but not patient records (unless also clinical role).

- **Session Timeout Policies:** BrightSmile Dental Group (Fictional) automatically logs out inactive users. Workstation screens lock after 5 minutes. Network devices timeout after 10 minutes. VPN sessions end after 30 minutes idle (12-hour maximum). EHR application times out after 10 minutes. Prevents abandoned sessions from being exploited.

- **Network Intrusion Detection Systems (NIDS) Controls:**
- **External Network Intrusion Detection System:** BrightSmile Dental Group (Fictional) deploys a sensor between internet connection and firewall that monitors all traffic entering/leaving the network. Uses 50,000+ attack signatures plus behavioral analysis to detect threats. Operates in stealth mode (invisible to attackers). Catches malware, exploits, reconnaissance attempts, and data theft.
- **24/7 Security Monitoring by CNDSP:** BrightSmile Dental Group (Fictional) contracts with Arctic Wolf Security Operations Center to monitor alerts around the clock. Expert analysts review all security events, filtering false alarms. Critical threats trigger phone call within 15 minutes. Service includes incident response support and annual penetration testing.
- **Internal Network Intrusion Detection System:** BrightSmile Dental Group (Fictional) operates a sensor connected to core switch that monitors all internal communications. Detects insider threats, compromised workstations, lateral movement between systems, and internal port scanning. Operates in stealth mode (no IP address, invisible on network).
- **Internal NIDS Stealth Mode Configuration:** BrightSmile Dental Group (Fictional) configures the monitoring system with two network cards. First card has no IP address and captures all traffic invisibly. Second card connects to management network for alerts and administration. Attackers cannot see or target the intrusion detection system.

- **Switches and VLANs Controls:**
- **VLAN Segmentation Strategy:** BrightSmile Dental Group (Fictional) divides the network into six isolated virtual networks. Clinical VLAN for treatment computers. Management VLAN for device administration. Server VLAN for EHR/files. Guest WiFi VLAN for patient internet with zero internal access. Admin VLAN for front desk. Unused VLAN (999) for disabled ports.
- **Access Control Lists Between VLANs:** BrightSmile Dental Group (Fictional) enforces firewall rules between network segments on the core switch. Clinical can access servers on HTTPS only. Guest completely blocked from internal systems. Management restricted to one administrator. All traffic denied by default unless specifically allowed. Violations are logged.
- **Port Security with MAC Address Filtering:** BrightSmile Dental Group (Fictional) locks each switch port to specific device MAC addresses. Unknown devices attempting connection cause port to shut down automatically with orange LED warning. SNMP alert sent to IT immediately. Prevents "plug in unauthorized laptop" attacks.
- **802.1X Port-Based Network Access Control:** BrightSmile Dental Group (Fictional) requires users to enter username/password before network jack activates. Credentials validated against RADIUS server. Users assigned to appropriate VLAN based on role. Failed attempts are logged. Prevents unauthorized use of wall jacks even with physical access.
- **Disabled Ports Assigned to Unused VLAN:** BrightSmile Dental Group (Fictional) assigns all unused switch ports to VLAN 999 (blackhole). This VLAN has no DHCP, no routing, no connectivity. Devices plugged into disabled ports get nothing. Any traffic detected triggers security alert.
- **Physical Switch Security:** BrightSmile Dental Group (Fictional) keeps all switches locked in cabinets requiring key/badge access. Only IT personnel authorized entry with sign-in log maintained. Prevents console port attacks since many switches can reset password with simple reboot. Security cameras monitor IT closet.

- **DHCP Snooping and Dynamic ARP Inspection:** BrightSmile Dental Group (Fictional) enables DHCP Snooping to prevent rogue DHCP servers by only trusting legitimate server port. Builds table of MAC-to-IP mappings. Dynamic ARP Inspection validates ARP packets against this table, dropping fakes. Prevents man-in-the-middle attacks on local network.

- **Virtual Private Network (VPN) Controls:**
- **IPsec VPN Gateway for Remote Access:** BrightSmile Dental Group (Fictional) operates an integrated VPN in the firewall allowing secure remote access for work-from-home staff. Uses military-grade AES-256 encryption. Users install client software, login with username/password/MFA token. Connected users assigned to isolated VPN subnet with limited access to internal resources.
- **Pre-Connection Device Compliance Checking:** BrightSmile Dental Group (Fictional) checks device security before allowing VPN connection. Verifies antivirus is updated (within 7 days), OS patches current (within 30 days), firewall enabled, disk encrypted. Devices failing checks are denied with remediation instructions.
- **Multi-Factor Authentication for VPN Access:** BrightSmile Dental Group (Fictional) requires VPN users to provide password PLUS second factor (mobile app code, push notification, or hardware token). Three failed attempts lock account. All attempts logged. Prevents remote access from stolen passwords alone.
- **VPN Session Management and Timeouts:** BrightSmile Dental Group (Fictional) auto-disconnects VPN sessions after 30 minutes idle or 12 hours maximum. All internet traffic must go through VPN tunnel (no split-tunneling). Kill switch blocks internet if VPN drops preventing unencrypted data leaks.
- **VPN Connection Monitoring and Logging:** BrightSmile Dental Group (Fictional) logs username, source location, connection time, data transferred, and resources accessed for all VPN sessions. Alerts generated for unusual activity: foreign countries, after-hours admin access, excessive downloads, multiple simultaneous sessions.
- **SSL VPN for Clientless Access:** BrightSmile Dental Group (Fictional) provides browser-based VPN for contractors/vendors without installing software. Users access web portal, authenticate with MFA, gain limited access to approved resources only. 15-minute timeout. All sessions logged with detailed tracking.

4.Database Security Risk Management Implementation Controls and Policies

- **Authentication – User Accounts:**
- **Multi-Factor Authentication (MFA):** BrightSmile Dental Group (Fictional) requires all employees to use MFA when accessing clinical and administrative systems, ensuring that even if passwords are stolen, unauthorized users cannot gain access.
- **Unique User IDs:** BrightSmile Dental Group (Fictional) assigns each staff member a unique account identifier to track individual actions and maintain accountability within all electronic systems.
- **Password Complexity Policy:** BrightSmile Dental Group (Fictional) enforces strong password policies, requiring long, complex passwords that must be changed every 90 days to prevent brute-force or reuse attacks.

- **Authorization:**
- **Role-Based Access Control (RBAC):** BrightSmile Dental Group (Fictional) grants access based on job roles, ensuring that staff only interact with data necessary for their duties, reducing exposure of sensitive information.

- **Principle of Least Privilege (PoLP):** BrightSmile Dental Group (Fictional) limits user privileges so that each employee has only the minimum access required, lowering insider and accidental data risk.
- **Access Review and Revocation:** BrightSmile Dental Group (Fictional) conducts quarterly access reviews and immediately revokes credentials for employees who leave or change positions.

- **Confidentiality:**
- **Data Encryption (AES-256):** BrightSmile Dental Group (Fictional) encrypts all patient and financial data using AES-256 and TLS 1.3 to ensure data cannot be intercepted or read by unauthorized parties.
- **Secure Email Gateway:** BrightSmile Dental Group (Fictional) uses HIPAA-compliant encrypted email for communication containing patient health information, ensuring confidentiality across networks.
- Privacy Screens and Physical Safeguards: BrightSmile Dental Group (Fictional) installs privacy screens and enforces workstation lockouts to prevent patients or visitors from viewing sensitive data.

- **Data Integrity:**
- **Digital Signatures:** BrightSmile Dental Group (Fictional) digitally signs patient forms and treatment records to authenticate origin and prevent tampering.
- **File Integrity Monitoring (FIM):** BrightSmile Dental Group (Fictional) monitors critical system files for unauthorized changes, ensuring early detection of manipulation or compromise.
- **Audit Trails:** BrightSmile Dental Group (Fictional) maintains detailed logs showing who accessed or modified data, supporting forensic investigations and compliance reviews.

- **Auditing:**
- **Security Information and Event Management (SIEM):** BrightSmile Dental Group (Fictional) integrates system logs into a SIEM platform that detects suspicious activities in real time.
- **Regular Audit Reviews:** BrightSmile Dental Group (Fictional) performs monthly reviews of access logs and system activity to identify policy violations or intrusion attempts.
- **Compliance Audits:** BrightSmile Dental Group (Fictional) undergoes annual third-party HIPAA and cybersecurity compliance audits to verify policy effectiveness.

- **Replication and Federation:**
- **Encrypted Data Replication:** BrightSmile Dental Group (Fictional) replicates data securely between local and cloud servers using encrypted channels to maintain confidentiality and availability.
- **Federated Authentication:** BrightSmile Dental Group (Fictional) uses single sign-on (SSO) to allow users to securely access multiple platforms with centralized credential management.
- **Redundant Systems:** BrightSmile Dental Group (Fictional) maintains mirrored servers that automatically synchronize data for uninterrupted operations.

- **Clustering:**
- **High Availability Clusters:** BrightSmile Dental Group (Fictional) uses clustered servers to ensure critical systems like patient management remain operational during hardware failures.
- Secure Node Communication: BrightSmile Dental Group (Fictional) authenticates each server node with digital certificates, protecting cluster communication from tampering.
- **Load Balancing:** BrightSmile Dental Group (Fictional) balances incoming requests across multiple systems to improve performance and reduce downtime risk.

- **Backup and Recovery:**
- **Daily Encrypted Backups**: BrightSmile Dental Group (Fictional) performs automated daily backups of critical systems, encrypting all data to protect it during storage and transfer.
- Offsite and Cloud Storage: BrightSmile Dental Group (Fictional) stores backups securely in both cloud environments and offsite facilities to ensure recovery during disasters.
- **Disaster Recovery Testing:** BrightSmile Dental Group (Fictional) conducts semi-annual recovery drills to verify the effectiveness of its backup and restoration procedures.

- **OS Protections:**
- **Patch Management**: BrightSmile Dental Group (Fictional) updates all operating systems monthly to address vulnerabilities and ensure system resilience.
- **Endpoint Detection and Response (EDR):** BrightSmile Dental Group (Fictional) deploys EDR solutions to detect and contain malware, ransomware, and other endpoint threats.
- **System Hardening:** BrightSmile Dental Group (Fictional) disables unnecessary services, default accounts, and open ports to minimize the attack surface.

- **Application Protections:**
- **Web Application Firewall (WAF):** BrightSmile Dental Group (Fictional) protects its online patient portal using a WAF to block SQL injection and cross-site scripting attacks.
- **Input Validation:** BrightSmile Dental Group (Fictional) enforces strict input validation in all software forms to prevent malicious data from being processed.
- **Code Review and Testing:** BrightSmile Dental Group (Fictional) reviews and tests all applications for vulnerabilities before deployment to production systems.

- **Network Protections:**
- **Next-Generation Firewall (NGFW):** BrightSmile Dental Group (Fictional) uses NGFWs to inspect network traffic and block unauthorized or malicious connections.
- **Network Segmentation:** BrightSmile Dental Group (Fictional) divides its network into isolated VLANs separating guest Wi-Fi, administrative, and clinical systems for better security.
- Intrusion Detection and Prevention (IDS/IPS): BrightSmile Dental Group (Fictional) monitors network traffic through IDS/IPS solutions that automatically block suspicious activity.

- **Security Design and Configuration:**
- **Security Baseline Configurations:** BrightSmile Dental Group (Fictional) deploys all new systems using CIS benchmarked secure configurations to maintain uniform protection.
- **Change Control Procedures:** BrightSmile Dental Group (Fictional) documents and reviews all system changes to prevent misconfigurations or unauthorized modifications.
- **Defense-in-Depth Architecture:** BrightSmile Dental Group (Fictional) layers controls across network, application, and user levels to minimize single points of failure.

- **Enclave and Computing Environment:**
- **Secure Clinical Network:** BrightSmile Dental Group (Fictional) isolates its clinical network from general business systems to protect patient data from exposure.
- **VPN Access:** BrightSmile Dental Group (Fictional) allows remote employees to connect through a secure VPN protected by encryption and MFA.
- Endpoint Protection Policies: BrightSmile Dental Group (Fictional) enforces antivirus, firewall, and encryption policies on all laptops and tablets used in the practice.

- **Business Continuity:**
- **Business Continuity Plan (BCP):** BrightSmile Dental Group (Fictional) maintains a documented BCP detailing how operations continue during system outages or emergencies.
- **Redundant Internet Connections:** BrightSmile Dental Group (Fictional) uses two separate ISPs to ensure continued access to cloud-based systems.
- **Power Backup Systems:** BrightSmile Dental Group (Fictional) installs UPS devices and generators to maintain essential operations during power disruptions.

- **Vulnerability and Incident Management:**
- **Vulnerability Scanning:** BrightSmile Dental Group (Fictional) performs quarterly vulnerability scans to identify and mitigate security risks.
- **Incident Response Plan (IRP):** BrightSmile Dental Group (Fictional) IRP defines detection, containment, and recovery processes for all security incidents.
- **Post-Incident Analysis:** BrightSmile Dental Group (Fictional) conducts detailed reviews after each incident to strengthen defenses and update policies accordingly.

5.Applications Development Security Risk Management Implementation Controls and Policies

- **Application Data Handling:**
- BrightSmile Dental Group (Fictional) ensures that all patient and business data is classified and handled according to its sensitivity level to maintain confidentiality and comply with HIPAA regulations.
- BrightSmile Dental Group (Fictional) encrypts all sensitive patient records both in transit using TLS 1.3 and at rest using AES-256 to protect against unauthorized access or data loss.
- BrightSmile Dental Group (Fictional) enforces strict access controls, allowing only authorized staff and providers to view or modify sensitive information within the dental management system.

- **Authentication:**
- BrightSmile Dental Group (Fictional) implements multi-factor authentication (MFA) across critical systems to ensure that staff identities are verified using at least two forms of credentials.
- BrightSmile Dental Group (Fictional) enforces a strong password policy requiring complex passwords, regular updates, and protection against reuse to enhance account security.
- BrightSmile Dental Group (Fictional) deploys automatic account lockout mechanisms after multiple failed login attempts to prevent brute-force or automated password attacks.
- BrightSmile Dental Group (Fictional) sets system session timeouts to automatically log out inactive users and reduce the risk of unauthorized access to patient data.

- **Use of Cryptography:**
- BrightSmile Dental Group (Fictional) employs industry-approved cryptographic algorithms such as AES and RSA to protect the confidentiality and integrity of patient and business data.
- BrightSmile Dental Group (Fictional) securely manages encryption keys using approved key vaults and rotates them regularly to prevent key compromise.
- BrightSmile Dental Group (Fictional) uses digital signatures on important documents and communications to ensure authenticity and prevent tampering.
- BrightSmile Dental Group (Fictional) maintains valid SSL/TLS certificates for its web services to guarantee secure communication with patients and partners.
- BrightSmile Dental Group (Fictional) conducts periodic cryptographic audits to ensure that all encryption methods remain up to date and compliant with HIPAA security standards.

- **User accounts:**
- BrightSmile Dental Group (Fictional) implements role-based access control (RBAC) so that each staff member can access only the information necessary to perform their specific job duties.
- BrightSmile Dental Group (Fictional) enforces the principle of least privilege, limiting administrative privileges to only essential personnel.
- BrightSmile Dental Group (Fictional) continuously monitors user activity and logs account actions to detect and respond quickly to suspicious behavior.
- BrightSmile Dental Group (Fictional) maintains a documented account management policy to ensure accountability and traceability of all access changes.

- **Input validation:**
- BrightSmile Dental Group (Fictional) validates all user input across applications to protect against injection attacks such as SQL injection and cross-site scripting.
- BrightSmile Dental Group (Fictional) implements both client-side and server-side input validation to reinforce security consistency and reliability.
- BrightSmile Dental Group (Fictional) encodes all user-generated output to prevent malicious scripts from executing within web applications.

- **Auditing:**
- BrightSmile Dental Group (Fictional) maintains comprehensive audit logs that capture all access, authentication, and modification activities across its systems.
- BrightSmile Dental Group (Fictional) ensures that audit logs are stored securely and are protected against unauthorized alteration or deletion.
- BrightSmile Dental Group (Fictional) regularly reviews system logs to identify abnormal access patterns, potential insider threats, or unauthorized data usage.
- BrightSmile Dental Group (Fictional) conducts internal audits quarterly to ensure continued compliance with HIPAA and other regulatory standards.

- **Configuration Management:**
- BrightSmile Dental Group (Fictional) maintains standardized, approved configuration baselines for all servers, workstations, and dental software systems.
- BrightSmile Dental Group (Fictional) follows a formal change control process that requires managerial approval for any system modifications.
- BrightSmile Dental Group (Fictional) applies timely security patches and software updates to address vulnerabilities and maintain operational stability.
- BrightSmile Dental Group (Fictional) performs regular configuration scans to verify that systems align with security benchmarks and policy requirements.
- BrightSmile Dental Group (Fictional) documents all configuration changes for accountability, traceability, and disaster recovery preparedness.

- **Testing:**
- BrightSmile Dental Group (Fictional) performs routine vulnerability scans and penetration tests on its software systems to detect and address security weaknesses.
- BrightSmile Dental Group (Fictional) uses static application security testing (SAST) to review source code and identify vulnerabilities before deployment.
- BrightSmile Dental Group (Fictional) conducts dynamic testing (DAST) to simulate real-world threats and ensure that applications can withstand common attack methods.

- BrightSmile Dental Group (Fictional) performs regression testing after system updates or patches to confirm that existing security controls remain effective.
- BrightSmile Dental Group (Fictional) integrates automated security testing into its development lifecycle to maintain consistent protection during software updates.

- **Deployment:**
- BrightSmile Dental Group (Fictional) uses a secure deployment pipeline that includes code verification, approval, and digital signing before release to production systems.
- BrightSmile Dental Group (Fictional) maintains strict separation between development, testing, and production environments to prevent data contamination and unauthorized access.
- BrightSmile Dental Group (Fictional) enforces change management approvals before any system is deployed or updated to ensure security validation and compliance.
- BrightSmile Dental Group (Fictional) monitors all deployed systems in real time to detect vulnerabilities, suspicious activities, or performance issues.
- BrightSmile Dental Group (Fictional) maintains a formal incident response plan that enables the team to respond quickly and effectively to any post-deployment security incidents.

6. Wireless Security Risk Management Implementation Controls and Policies

- **Wireless LAN (WLAN) Risk Management:**
- **WPA3/WPA2-Enterprise Encryption:** BrightSmile Dental Group (Fictional) uses WPA3/WPA2-Enterprise encryption to protect the staff wireless network, ensuring that only authorized employees and approved clinical devices can connect. This prevents attackers from intercepting or manipulating wireless traffic inside the clinic.
- **Staff and Guest Network Segmentation:** BrightSmile Dental Group (Fictional) separates its wireless networks into staff and guest VLANs to ensure patient visitors cannot access internal systems. This segmentation reduces the attack surface and prevents unauthorized devices from reaching sensitive clinical resources.
- **SSID Security Controls:** BrightSmile Dental Group (Fictional) uses a non-identifiable SSID and limits broadcast visibility to cut down on wireless reconnaissance attempts. This helps prevent attackers from easily locating or targeting the clinic's internal wireless network.

- **2.Wireless PAN (WPAN) Risk Management:**
- **Secure Bluetooth Pairing:** BrightSmile Dental Group (Fictional) configures its Bluetooth-enabled clinical tools to use secure pairing methods that require authentication. This guarantees that only approved devices like intraoral cameras or scanners can connect and stops unauthorized proximity attacks.
- **Non-Discoverable Device Configuration:** BrightSmile Dental Group (Fictional) sets Bluetooth devices to operate in non-discoverable mode unless pairing is necessary. This reduces the chances that external attackers can detect and target clinical equipment.
- **Regular Firmware Updates:** BrightSmile Dental Group (Fictional) makes sure all Bluetooth and short-range wireless devices get regular firmware updates. Keeping devices updated shields them from known Bluetooth vulnerabilities and exploits.

- **3. Wireless WAN (WWAN) Risk Management:**
- **VPN for Mobile Access:** BrightSmile Dental Group (Fictional) requires staff to use a secure VPN when accessing clinic systems over cellular networks like 4G or 5G. This ensures sensitive data, including appointment schedules or patient info, remains encrypted and protected from interception.
- **Mobile Device Management (MDM):** BrightSmile Dental Group (Fictional) enrolls approved mobile devices into an MDM system that enforces encryption, strong authentication, and remote-

wipe features. This safeguards patient data if a device is lost, stolen, or compromised outside the office.

- **Hotspot Restrictions:** BrightSmile Dental Group (Fictional) disables hotspot and tethering functions on clinic-owned devices to prevent the creation of unauthorized wireless access points. This lowers the risk of unintentional exposure to attackers who might connect to insecure hotspots.

- **4. Wireless RFID Risk Management:**
- **Encrypted Staff Badges:** BrightSmile Dental Group (Fictional) uses encrypted RFID access badges to ensure employee credentials cannot be cloned or duplicated. This prevents unauthorized individuals from gaining physical access to restricted areas such as server rooms or records storage.
- **Controlled RFID Reader Power Levels:** BrightSmile Dental Group (Fictional) sets RFID readers with limited broadcast power so badge scans can't be intercepted from outside the building. This defends the clinic against long-range RFID skimming attempts.
- **Immediate Badge Deactivation:** BrightSmile Dental Group (Fictional) promptly deactivates any lost or inactive RFID badges once reported. This stops unauthorized entry using misplaced or stolen access cards.

- **5. Wireless PED (Portable Electronic Device) Risk Management:**
- **Full-Device Encryption:** BrightSmile Dental Group (Fictional) requires all smartphones, tablets, and laptops used for clinic operations to have full disk encryption. This ensures patient info and business data stay protected if a device is lost or stolen.
- **Strong Authentication & Auto-Lock:** BrightSmile Dental Group (Fictional) enforces strong authentication methods such as PINs, biometrics, and automatic screen-locking on all PEDs. This prevents unauthorized access to sensitive data when a device is unattended.
- **BYOD Security Policy:** BrightSmile Dental Group (Fictional) mandates that personal devices meet security standards, including system updates, encryption, and screen locks, before connecting to the staff wireless network. This policy helps prevent insecure personal devices from introducing malware or vulnerabilities into the clinic environment.

b) Comparison of the Implementation controls discussed in class with your company's existing Cybersecurity Implementation controls

Cybersecurity Controls	Control Type	BrightSmile Dental Group (Fictional) Status
Identification Credentials		
Employee ID Number	Access Control Security	Implemented
Username/User ID	Access Control Security	Implemented
Email Address	Access Control Security	Implemented
Professional License Numbers	Access Control Security	Implemented
Social Security Number (SSN)	Access Control Security	Implemented
Digital Certificates	Access Control Security	No Implemented
Social Security Number (SSN)	Access Control Security	Implemented
NPI(National Provider Identifier)	Access Control Security	Implemented
API Keys/Access Tokens	Access Control Security	No Implemented
Domain Account Credentials	Access Control Security	No Implemented
Vendor/Contractor ID	Access Control Security	No Implemented
Personal Authorization		
Password Authentication	Access Control Security	Implemented
PIN (Personal Identification Number)	Access Control Security	Implemented
Security Questions	Access Control Security	Implemented

Multi-Factor Authentication (MFA)	Access Control Security	Partially Implemented
Biometric Authentication	Access Control Security	No Implemented
Smart Card/Badge Authentication:	Access Control Security	No Implemented
Hardware Security Keys (FIDO Keys)	Access Control Security	No Implemented
Mobile Push Notifications	Access Control Security	No Implemented
Time-Based One-Time Passwords (TOTP)	Access Control Security	No Implemented
Certificate-Based Authentication	Access Control Security	No Implemented
Risk-Based/Adaptive Authentication	Access Control Security	No Implemented
Privileged Access Management (PAM)	Access Control Security	No Implemented
Authorization		
Role-Based Access Control (RBAC)	Access Control Security	Implemented
Least Privilege Principle	Access Control Security	Implemented
Access Control Lists (ACLs)	Access Control Security	Implemented
Discretionary Access Control (DAC)	Access Control Security	Partially Implemented
Attribute-Based Access Control (ABAC)	Access Control Security	No Implemented
Mandatory Access Control (MAC)	Access Control Security	No Implemented
Logical Access Control Methods		
Password Authentication	Access Control Security	Implemented
Encryption	Access Control Security	Implemented
Session Timeouts	Access Control Security	Implemented
Account Lockout Policies	Access Control Security	Implemented
Firewalls	Access Control Security	Implemented
Virtual Private Networks (VPNs)	Access Control Security	Partially Implemented
Single Sign-On (SSO)	Access Control Security	No Implemented
Physical Access Control Methods		
Locks and Keys	Access Control Security	Implemented
Alarm Systems	Access Control Security	Implemented
CCTV/Surveillance Cameras	Access Control Security	Implemented
Visitor Management	Access Control Security	Implemented
Motion Detectors	Access Control Security	Implemented
Key Cards/Proximity Cards	Access Control Security	No Implemented
Smart Cards with PIN	Access Control Security	No Implemented
Mantrap/Airlock Doors	Access Control Security	No Implemented
Turnstiles and Gates	Access Control Security	No Implemented
Bollards and Barriers	Access Control Security	No Implemented
Security Guards	Access Control Security	No Implemented
Biometric Systems		
Fingerprint Scanners	Access Control Security	No Implemented
Facial Recognition	Access Control Security	No Implemented
Iris Scanning	Access Control Security	No Implemented
Retinal Scanning	Access Control Security	No Implemented
Voice Recognition	Access Control Security	No Implemented
Enclave Protection Controls		
Network Segmentation	Network Infrastructure Security	Implemented
Access Control Lists (ACLs)	Network Infrastructure Security	Implemented

Intrusion Detection/Prevention Systems (IDPS)	Network Infrastructure Security	Implemented
Server Hardening	Network Infrastructure Security	Implemented
Data Encryption	Network Infrastructure Security	Implemented
Micro-segmentation	Network Infrastructure Security	No Implemented
Zero Trust Architecture	Network Infrastructure Security	Partially Implemented
Least Privilege	Network Infrastructure Security	Implemented
Firewall Controls		
Default-Deny Policy	Network Infrastructure Security	Implemented
Stateful Inspection	Network Infrastructure Security	Implemented
Application Layer Filtering	Network Infrastructure Security	Implemented
Geographic Filtering	Network Infrastructure Security	No Implemented
Centralized Log and Audit	Network Infrastructure Security	Partially Implemented
Rule Minimization and Review	Network Infrastructure Security	Implemented
Router Controls		
Management Plane Hardening	Network Infrastructure Security	Partially Implemented
Strong Authentication & MFA	Network Infrastructure Security	Partially Implemented
Physical Security	Network Infrastructure Security	Implemented
Interface Access Control Lists (ACLs)	Network Infrastructure Security	Implemented
Regular Firmware Updates	Network Infrastructure Security	Partially Implemented
Anti-Spoofing Controls	Network Infrastructure Security	Implemented
Broadcast Suppression	Network Infrastructure Security	Implemented
Network Address Translation (NAT)	Network Infrastructure Security	Implemented
Logging & Monitoring	Network Infrastructure Security	Partially Implemented
Ports, Protocols, Services (PPS) Risk Management		
Access Lists	Network Infrastructure Management Security	Implemented
Network Access Control (NAC) Beyond 802.1X	Network Infrastructure Management Security	Partially Implemented
Device Risk Management		

Unicast Reverse Path Forwarding (uRPF)	Network Infrastructure Management Security	No Implemented
IP Address Management	Network Infrastructure Management Security	Implemented
Protecting Routers	Network Infrastructure Management Security	Implemented
Out-of-Band Management	Network Infrastructure Management Security	Implemented
In-Band Management	Network Infrastructure Management Security	Implemented
Router Password Protection	Network Infrastructure Management Security	Implemented
Device Monitoring, Network Management Risk Management		
SNMP	Network Infrastructure Management Security	Partially Implemented
Syslog Server	Network Infrastructure Management Security	Implemented
Network Authentication, Authorization, and Accounting Risk Management		
Individual User Account	Network Infrastructure Management Security	Implemented
Access Control	Network Infrastructure Management Security	Implemented
Network Intrusion Detection Risk Management (NIDS)		
LAN IDS	Network Infrastructure Management Security	Implemented
External IDS	Network Infrastructure Management Security	Implemented
Switches and VLANs Risk Management		
Protecting Servers and LANs	Network Infrastructure Management Security	Implemented
VLAN Technology	Network Infrastructure Management Security	Implemented
Port Security	Network Infrastructure Management Security	Implemented
IEEE 802.1X	Network Infrastructure Management Security	Implemented
VMPS for Dynamic VLAN Allocation	Network Infrastructure Management Security	No Implemented
DHCP Snooping	Network Infrastructure Management Security	Implemented
Dynamic ARP Inspection (DAI)	Network Infrastructure Management Security	Implemented
Routing Protocol Authentication	Network Infrastructure Management Security	No Implemented
Virtual Private Network Risk Management		
Gate-to-Gate VPN	Network Infrastructure Management Security	Implemented
Host-to-Gate VPN	Network Infrastructure Management Security	Implemented

Host-to-Host VPN	Network Infrastructure Management Security	No Implemented
Authentication -User Accounts		
Multi-Factor Authentication (MFA)	Database Security Risk Management	Implemented
Unique User IDs	Database Security Risk Management	Implemented
Password Complexity	Database Security Risk Management	Implemented
Authorization		
Role-Based Access Control (RBAC)	Database Security Risk Management	Implemented
Privileged Account Management	Database Security Risk Management	Implemented
Access Review and Termination Controls	Database Security Risk Management	Implemented
Principle of Least Privilege (PoLP)	Database Security Risk Management	Implemented
Confidentiality		
Data Encryption (AES-256)	Database Security Risk Management	Implemented
Encryption Tools and Key Management	Database Security Risk Management	Implemented
Secure Email Gateway	Database Security Risk Management	Partially Implemented
Data Integrity		
Digital Signatures	Database Security Risk Management	Implemented
File Integrity Monitoring (FIM)	Database Security Risk Management	Partially Implemented
Audit Trails	Database Security Risk Management	Implemented
Replication and Federation		
Security Information and Event Management (SIEM)	Database Security Risk Management	Implemented
Regular Audit Reviews	Database Security Risk Management	Partially Implemented
Compliance Audits	Database Security Risk Management	Implemented
Clustering		
Encrypted Data Replication	Database Security Risk Management	Implemented
Federated Authentication	Database Security Risk Management	Implemented
Redundant Systems	Database Security Risk Management	Implemented
Backup and Recovery		
Daily Encrypted Backups	Database Security Risk Management	Implemented

Offsite and Cloud Storage	Database Security Risk Management	Implemented
Disaster Recovery Testing	Database Security Risk Management	No Implemented
OS Protections		
Patch Management	Database Security Risk Management	Implemented
Endpoint Detection and Response (EDR)	Database Security Risk Management	Implemented
System Hardening	Database Security Risk Management	Implemented
Application Protections		
Web Application Firewall (WAF)	Database Security Risk Management	Implemented
Input Validation	Database Security Risk Management	Implemented
Code Review and Testing	Database Security Risk Management	Implemented
Network Protections		
Next-Generation Firewall (NGFW)	Database Security Risk Management	Implemented
Network Segmentation	Database Security Risk Management	Implemented
Intrusion Detection and Prevention (IDS/IPS)	Database Security Risk Management	Implemented
Security Design and Configuration		
Security Baseline Configurations	Database Security Risk Management	Implemented
Change Control Procedures	Database Security Risk Management	Implemented
Defense-in-Depth Architecture	Database Security Risk Management	Implemented
Enclave and Computing environment		
Secure Clinical Network	Database Security Risk Management	Implemented
VPN Access	Database Security Risk Management	Implemented
Endpoint Protection Policies	Database Security Risk Management	Implemented
Business Continuity		
Business Continuity Plan (BCP)	Database Security Risk Management	Implemented
Redundant Internet Connections	Database Security Risk Management	Implemented
Power Backup Systems	Database Security Risk Management	Implemented
Vulnerability and Incident management		
Vulnerability Scanning	Database Security Risk Management	Implemented

Incident Response Plan (IRP)	Database Security Risk Management	Implemented
Post-Incident Analysis	Database Security Risk Management	Implemented
Program Management		
Applications Development	Applications Development Security Risk Management	Implemented
Secure SDLC Oversight	Applications Development Security Risk Management	Implemented
Application Data Handling		
Data Encryption (AES-256, TLS 1.3)	Applications Development Security Risk Management	Implemented
Data Classification and Retention Policy	Applications Development Security Risk Management	Partially Implemented
Data Backup and Recovery Plan		Implemented
Authentication		
Multi-Factor Authentication (MFA)	Applications Development Security Risk Management	Implemented
Password Policy Enforcement	Applications Development Security Risk Management	Implemented
Single Sign-On (SSO) Integration	Applications Development Security Risk Management	Partially Implemented
Use of Cryptography		
Cryptographic Key Management	Applications Development Security Risk Management	Implemented
Digital Certificates (SSL/TLS)	Applications Development Security Risk Management	Implemented
Data Integrity Verification (Checksums, Hashing)	Applications Development Security Risk Management	Implemented
User Accounts		
Role-Based Access Control (RBAC)	Applications Development Security Risk Management	Implemented
Privileged Account Management (PAM)	Applications Development Security Risk Management	Implemented
User Provisioning and Deprovisioning	Applications Development Security Risk Management	Implemented
Input Validation		
Input Sanitization and Validation	Applications Development Security Risk Management	Implemented
Form Data Encryption and Encoding	Applications Development Security Risk Management	Implemented
Auditing		
Audit Logs and Monitoring	Applications Development Security Risk Management	Implemented
Configuration Management		
Patch Management and System Updates	Applications Development Security Risk Management	Implemented
Baseline Configuration Standards	Applications Development Security Risk Management	Implemented
Testing		

Vulnerability and Penetration Testing	Applications Development Security Risk Management	No Implemented
Static and Dynamic Application Security Testing (SAST/DAST)	Applications Development Security Risk Management	Implemented
Security Control Validation (Annual Audits)	Applications Development Security Risk Management	Implemented
Deployment		
Secure Software Deployment Procedures	Applications Development Security Risk Management	Implemented
Change Management and Approval Process	Applications Development Security Risk Management	Implemented
Separation of Development and Production Environments	Applications Development Security Risk Management	Implemented
Post-Deployment Review and Monitoring	Applications Development Security Risk Management	Partially Implemented
Wireless LAN Risk Management		
IEEE 802.11 WLAN Security Standard (WPA3/WPA2-Enterprise)	Wireless Security Risk Management	Implemented
SSID Hardening (Hidden SSID, Non-Identifiable Naming)	Wireless Security Risk Management	Partially Implemented
Network Segmentation (VLANs for Staff/Guest)	Wireless Security Risk Management	Implemented
Wireless Intrusion Detection / Prevention (WIDS/WIPS)	Wireless Security Risk Management	No Implemented
MAC Address Filtering	Wireless Security Risk Management	Implemented
Wireless PAN Risk Management		
Secure Bluetooth Pairing	Wireless Security Risk Management	Implemented
Bluetooth Non-Discoverable Mode	Wireless Security Risk Management	Implemented
Firmware / Bluetooth Patch Management	Wireless Security Risk Management	Partially Implemented
Bluetooth Proximity Monitoring (RSSI Monitoring)	Wireless Security Risk Management	No Implemented
Authorized Device Access Restrictions	Wireless Security Risk Management	Implemented
Wireless WAN Risk Management		
VPN Requirement for 4G/5G Connections	Wireless Security Risk Management	Implemented
Mobile Device Management (MDM)	Wireless Security Risk Management	Implemented
Hotspot / Tethering Restrictions	Wireless Security Risk Management	Implemented
Cellular Intrusion Detection (Rogue Femtocell Monitoring)	Wireless Security Risk Management	No Implemented
Remote Wipe Capability	Wireless Security Risk Management	Implemented
Wireless RFID Risk Management		

Encrypted RFID Access Badges (HF/UHF Security)	Wireless Security Risk Management	Implemented
Reduced RFID Signal Power Levels	Wireless Security Risk Management	Implemented
RFID Anti-Cloning Technology	Wireless Security Risk Management	Partially Implemented
RFID Access Log Monitoring & Alerting	Wireless Security Risk Management	Partially Implemented
Immediate Badge Deactivation Policy	Wireless Security Risk Management	Implemented
Wireless PED Risk Management		
Full-Device Encryption (AES-256)	Wireless Security Risk Management	Implemented
Strong Authentication + Auto-Lock	Wireless Security Risk Management	Implemented
BYOD Compliance Enforcement via MDM	Wireless Security Risk Management	Partially Implemented
Application Whitelisting	Wireless Security Risk Management	No Implemented
Blocking Unauthorized Wireless Adapters	Wireless Security Risk Management	No Implemented

c) Create a list of critical assets in $ that exist in your company

Total Estimated Practice Value Range: $1.5 Million - $5 Million+

Asset Name	Asset Value (Estimated)
IT & Data Assets	
Patient Electronic Health Records (EHR) Database	$500,000 - $2,000,000
Practice Management Software System	$15,000 - $50,000
Digital Imaging Software & Storage	$10,000 - $30,000
Backup Systems & Data Recovery	$5,000 - $15,000
Server Infrastructure	$10,000 - $25,000
Workstation Computers (per unit)	$1,000 - $2,500
Network Equipment (routers, switches, firewalls)	$5,000 - $15,000
Patient Portal System	$5,000 - $10,000
Clinical Equipment	
Digital X-Ray Systems (Panoramic)	$35,000 - $80,000
Digital Sensors (Intraoral X-ray)	$8,000 - $15,000 each
Dental Chairs (per unit)	$8,000 - $25,000
Dental Operatory Equipment (lights, delivery systems)	$5,000 - $15,000 per operatory
Intraoral Cameras	$1,500 - $4,000 each
Sterilization Equipment (Autoclave)	$3,000 - $8,000
Ultrasonic Cleaners	$1,000 - $3,000
Compressor Systems	$3,000 - $10,000

Suction Systems	$5,000 - $15,000
Handpieces (high-speed, low speed)	$1,000 - $3,000 each
Curing Lights	$500 - $2,000 each
Anesthesia Equipment	$2,000 - $5,000
Specialty Equipment	
CEREC/CAD-CAM System	$80,000 - $150,000
Cone Beam CT Scanner (CBCT)	$75,000 - $150,000
Laser Equipment (soft tissue, hard tissue)	$15,000 - $50,000
Nitrous Oxide System	$3,000 - $8,000
Office Infrastructure	
Office Space/Lease Improvements	$100,000 - $500,000
Reception Furniture & Waiting Room	$10,000 - $30,000
Office Furniture (desks, chairs, cabinets)	$15,000 - $40,000
Security System (cameras, alarms)	$3,000 - $10,000
Phone System	$2,000 - $8,000
Intangible Assets	
Patient List/Active Patient Base	$300,000 - $1,500,000
Reputation & Brand Value	$100,000 - $500,000
Insurance Contracts/Provider Networks	$50,000 - $200,000
Website & Online Presence	$5,000 - $20,000
Credentials & Licenses	
Professional Licenses (DEA, State Dental License)	Invaluable (legal requirement)
NPI Numbers	Invaluable (billing requirement)
Insurance Credentialing	$10,000 - $30,000 (cost to establish)

(d) List of potential vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing

Absent Cybersecurity Control	Potential Vulnerabilities
Access Control Risk Management	
Digital Certificates	Man-in-the-middle attacks can intercept communications. Software and email sources cannot be verified as authentic. Phishing attacks appear legitimate. Data transmission remains unencrypted and exposed. Spoofed websites and applications deceive users.
API Keys/Access Tokens	Unauthorized access to cloud services occurs. Third-party integrations lack secure credential management. Access to connected systems cannot be effectively revoked. Automated communications lack audit trails. Credentials in configuration files are exposed to attackers.
Domain Account Credentials	Account management across systems is decentralized and inconsistent. Password policies vary across platforms. Access revocation is delayed when employees leave. Local administrator accounts remain unmanaged. Audit logging is fragmented across systems.

Vendor/Contractor ID	Third parties use employee credentials. External workers gain unrestricted internal access. Access controls are not time limited. External activity cannot be distinguished from internal. Access continues after contracts end.
Biometric Authentication	Credentials are shared between users. User identity cannot be definitively proven. Passwords are stored insecurely. Users can deny they accessed systems. Compromised credentials grant immediate full access.
Smart Card/Badge Authentication	Single-factor authentication is insufficient for sensitive systems. Remote access lacks physical security tokens. Physical and logical access cannot be disabled simultaneously. Critical resources rely on password-only access. Physical and digital access systems are not integrated.
Hardware Security Keys (FIDO Keys)	Sophisticated phishing attacks succeed. User presence cannot be cryptographically proven. Privileged accounts are vulnerable to credential theft. SMS authentication is vulnerable to SIM swapping. Real-time phishing bypasses traditional MFA.
Mobile Push Notifications	Unauthorized access attempts are not immediately detected. SMS codes are intercepted or delayed. Users lack contextual information during authentication. Fraudulent login detection is delayed. Suspicious access cannot be easily denied.
Time-Based One-Time Passwords (TOTP)	Static passwords remain valid indefinitely. Credential stuffing attacks succeed with breached databases. Compromise windows are extended without rotating codes. Stored passwords remain usable by attackers. Replay attacks succeed if credentials are intercepted.
Certificate-Based Authentication	Remote network access relies on passwords only. Device-level authentication is not required. Wireless access uses shared passwords. Stolen credentials grant immediate network access. Device compliance cannot be enforced.
Risk-Based/Adaptive Authentication	Unusual geographic logins go undetected. Abnormal access times are not flagged. Compromised accounts operate undetected for long periods. Suspicious patterns receive no automated response. Authentication requirements do not adjust to risk.
Privileged Access Management (PAM)	Permanent administrative credentials remain in use. Privileged passwords are shared among administrators. Administrative activities are not monitored or recorded. Elevated privileges never expire. Administrative passwords are stored insecurely.

Attribute-Based Access Control (ABAC)	Multiple passwords create user fatigue. Password reuse occurs across systems. Weak passwords are chosen due to complexity burden. Multiple logins reduce workflow efficiency. Centralized access revocation is difficult.
Mandatory Access Control (MAC)	Permissions remain static regardless of context. Time-based or location-based restrictions are absent. Permissions do not adjust with role changes. Temporary users receive overly broad access. Contextual need-to-know cannot be enforced.
Single Sign-On (SSO)	Formal data classification systems are absent. Access is uniform regardless of sensitivity. Financial and operational data are not segregated. Clearance-based enforcement does not exist. Sensitive information lacks mandatory protection.
Key Cards/Proximity Cards	Physical keys can be copied or lost. Facility entry and exit cannot be tracked. Access cannot be remotely disabled. Lock replacement is expensive when compromised. Facility access audit trails do not exist.
Smart Cards with PIN	Single-factor physical access is insufficient. Lost credentials grant immediate access. Credential holders cannot be identity verified. Physical credentials are shared among users. Unauthorized duplication cannot be prevented.
Mantrap/Airlock Doors	Tailgating into restricted areas goes undetected. Multiple entries occur on single authentication. One-person authentication is not physically enforced. Visitors bypass security checkpoints. Piggybacking through secure doors cannot be prevented.
Turnstiles and Gates	Multiple people enter on single credentials. Entry points can be bypassed. Authorized entries are not physically counted. Access control points lack enforcement. Unrestricted movement occurs in secure areas.
Bollards and Barriers	Facilities are vulnerable to vehicle-based attacks. Forced entry by vehicles is not prevented. Vehicle access to restricted areas is uncontrolled. Ram-raiding and vehicle theft become possible. Physical perimeters are easily breached.
Security Guards	Identities at entry points are not verified. Suspicious activity goes unobserved. Security incident response is delayed. Visible security deterrents are absent. After-hours incidents remain undetected.
Fingerprint Scanners	Credentials are shared between individuals. Biological proof of identity is absent. User actions cannot be definitively proven. Users can deny

	access events. Accountability for sensitive operations is weak.
Facial Recognition	Continued user presence is not verified. Authenticated sessions are used by unauthorized individuals. Continuous authentication is lacking. Disguises and obfuscation are not detected. Physical presence is not required for authentication.
Iris Scanning	High-value assets lack strongest authentication. Critical operations lack near-impossible-to-forge verification. Sensitive areas are accessible with weaker credentials. Protection is inadequate for highest security needs. Shared access to critical resources occurs.
Retinal Scanning	Ultra-high-value transactions lack strongest verification. Critical financial operations use weak authentication. Extremely sensitive information is accessible with passwords. Medical-grade identity verification is unavailable. Non-repudiation is insufficient for critical operations.
Voice Recognition	Phone authentication is easily spoofed. Verbal authorizations lack biometric verification. Remote identity verification has significant weaknesses. Impersonation succeeds over communication systems. Voice-based access controls are completely absent.
Network Infrastructure Security Risk Management	
Micro-segmentation	Lateral Movement of Malware**.** If a workstation on the Clinical VLAN is infected (e.g., via a malicious email), the malware could spread unimpeded to other critical systems on the same VLAN, such as the database server or other chairside computers.
Continuous Zero Trust Validation	Insider Threat & Credential Compromise. Once a user is authenticated, their session is typically trusted. A logged-in workstation left unattended could be misused. A stolen password could be used to access PHI from any internal device without further checks.
Formal Rule Set Review	Policy Drift & Accidental Exposure**.** Over time, firewall rules may become overly permissive to solve temporary problems, creating permanent weaknesses. An unused rule could accidentally expose a sensitive system to a less-trusted network.
Geographic Filtering	Targeted Attacks from High-Risk Regions. The practice is exposed to brute-force attacks, scans, and exploit attempts originating from countries where there is no business need for connectivity.
Centralized Logging (SIEM)	Undetected Intrusions & Slow Incident Response. Without correlating logs from the firewall, EDR, and other systems, sophisticated attacks that leave subtle

	traces across different systems will go undetected. Investigating a security incident is slow and manual.
Strict Firmware Update Schedule	Exploitation of Known Vulnerabilities. Network devices (firewall, switch) often have published vulnerabilities. Without a formal process for prompt patching, the practice is exposed to attacks that exploit these known weaknesses to compromise the network core.
MFA on All Network Device Logins	Unauthorized Configuration Changes. If an attacker guesses or phishes a network admin's password, they could log into the switch or firewall and change settings to weaken security, create backdoors, or disrupt network operations.
Data Loss Prevention (DLP)	Accidental or Malicious PHI Theft. There is no technical control to prevent a staff member from emailing a patient file to a personal account, uploading a patient list to a cloud storage service, or copying data to a USB drive.
Strict Application Whitelisting	Execution of Unauthorized Software. While EDR is good, it is reactive. A user could accidentally run a crypto miner, ransomware, or other unauthorized software that is not yet recognized as malicious by the EDR.
Network Infrastructure Management Security Risk Management	
Unicast Reverse Path Forwarding (uRPF)	Without uRPF, attackers can spoof source IP addresses to bypass firewall ACLs and impersonate trusted systems. External attackers forge internal IP addresses to evade security policies. The network can be exploited as a DDoS amplifier using spoofed packets. Attackers hide their true origin making forensic investigation difficult.
SNMP	Limited SNMP monitoring reduces network visibility and delays problem detection. Performance issues go unnoticed until users complain. Interface errors remain undetected until complete failure. No bandwidth trending prevents capacity planning. Configuration drift and unauthorized changes may go undetected. Troubleshooting is reactive rather than proactive.
VMPS for Dynamic VLAN Allocation	No vulnerabilities exist when 802.1X is implemented instead. 802.1X uses credential-based authentication which is more secure than VMPS's MAC-based approach. Current implementation is superior to VMPS technology.
Host-to-Host VPN	Internal communications travel unencrypted exposing sensitive data to network eavesdropping. Attackers with internal access can use packet sniffers to capture confidential communications. Man-in-the-middle attacks can intercept traffic between internal hosts. Compromised workstations

	can monitor administrative traffic. Insider threats can eavesdrop on executive discussions without detection.
Routing Protocol Authentication	No vulnerabilities exist when dynamic routing protocols are not in use. Single-site networks using static routing do not require routing protocol authentication. No routing advertisements exist to spoof or manipulate.
Network Access Control (NAC) Beyond 802.1X	Non-compliant devices can access the network with valid credentials alone. Outdated workstations with missing patches connect if password is correct. Devices with disabled antivirus or expired signatures gain access. No continuous monitoring during active sessions. BYOD devices not comprehensively assessed. No automated quarantine for non-compliant devices. IoT devices lack automated policy enforcement.
Database Security Risk Management	
Replication and Federation	Lack of real-time replication could cause data loss or inconsistency between on-premise and cloud systems during outages or ransomware incidents. Absence of single sign-on (SSO) or federated identity may result in weak authentication and credential sprawl, increasing the risk of compromised logins. Limited synchronization monitoring could expose replication channels to data interception or corruption.
Policy Implementations	Infrequent policy reviews can cause outdated security configurations, leaving systems noncompliant with new regulations. Missing employee acknowledgment tracking could lead to unawareness of security responsibilities. Weak policy enforcement increases the likelihood of inconsistent control application across departments.
Network Protections	Partial Zero-Trust implementation leaves internal lateral movement paths open for attackers after initial compromise. Missing micro-segmentation increases the risk of ransomware propagation. Limited IDS/IPS tuning may cause delayed detection of malicious traffic.
Enclave and Computing Environment	Limited virtualization and compliance monitoring allow unmanaged devices or unpatched endpoints to connect to sensitive systems. Insufficient endpoint isolation can lead to malware spread across enclaves. Weak monitoring can delay detection of unauthorized access attempts.
Security Awareness and Training	Employees may fall for phishing attacks or social engineering, resulting in credential theft. Poor awareness can lead to insecure handling of patient data (e.g., sharing over unencrypted email). Failure

	to report suspicious activity increases incident response delays.
Applications Development Security Risk Management	
Data Classification and Retention Policy	Lack of automated data classification and retention tracking increases the risk of sensitive data being mishandled or stored insecurely. Without defined retention limits, confidential records may be retained longer than necessary, heightening exposure in a breach.
Secure Data Disposal	Improper or manual data disposal methods can leave recoverable traces of sensitive information on devices or media. This increases the likelihood of data leaks and regulatory violations during device retirement or recycling.
Single Sign-On (SSO) Integration	The absence of SSO forces users to manage multiple passwords, encouraging weak or reused credentials. Disconnected authentication systems make centralized monitoring and password enforcement more difficult.
Cryptographic Key Management	Manual key management increases the risk of key exposure, weak encryption practices, and expired certificates. Without automated rotation and centralized storage, attackers could exploit compromised keys for prolonged access.
User Provisioning and Deprovisioning	Manual account management can result in orphaned or excessive user privileges after employee turnover. This creates opportunities for unauthorized access and insider misuse of systems.
Input Sanitization and Validation	Insufficient input validation allows attackers to inject malicious commands or scripts into applications. Such vulnerabilities can lead to data corruption, unauthorized access, or system compromise.
Baseline Configuration Standards	Inconsistent or unmonitored system configurations create opportunities for misconfigurations and default credentials to persist. This increases the attack surface and weakens overall network security.
Vulnerability and Penetration Testing	Without regular testing, undetected software flaws and configuration weaknesses remain exploitable. The absence of assessments limits the ability to identify and remediate emerging threats.
Static and Dynamic Application Security Testing (SAST/DAST)	Lack of code-level and runtime testing leaves applications vulnerable to hidden programming and configuration flaws. Missing security scans can allow injection or API vulnerabilities to reach production.
Post-Deployment Review and Monitoring	Failure to conduct post-deployment reviews delays the detection of new vulnerabilities or configuration issues. Unmonitored changes increase the risk of breaches and hinder rapid incident response.

Wireless Security Risk Management	
SSID Hardening (Hidden SSID, Non-Identifiable Naming)	Without SSID hardening, attackers can easily identify the wireless network belonging to a business and target it for credential cracking or impersonation attacks. A visible or descriptive SSID enables attackers to harvest information about the organization and potentially spoof the network to capture user credentials.
Wireless Intrusion Detection / Prevention (WIDS/WIPS)	Without WIDS/WIPS, rogue access points, evil twin attacks, and unauthorized Wi-Fi devices can operate undetected within radio range. Attackers can intercept traffic, perform man-in-the-middle attacks, or bypass perimeter defenses without the organization ever being alerted.
MAC Address Filtering	If MAC filtering is not implemented, unauthorized devices can more easily connect to the network, increasing the risk of internal reconnaissance and lateral movement. Attackers may exploit open access to inject malicious traffic, capture sensitive data, or launch attacks from within the trusted network.
Firmware / Bluetooth Patch Management	Unpatched Bluetooth devices remain vulnerable to known exploits such as BlueBorne, allowing attackers to take control of devices or intercept data. Outdated firmware creates an attack surface that threat actors can exploit to compromise dental equipment or breach patient information.
Bluetooth Proximity Monitoring (RSSI Monitoring)	Without proximity monitoring, attackers can stay within Bluetooth range unnoticed and attempt unauthorized pairing or signal injection. This increases risks of device hijacking, data interception, or unauthorized wireless connections near the facility.
Hotspot / Tethering Restrictions	If hotspot restrictions are not enforced, staff or visitors can create unmanaged network paths that bypass corporate security controls. These shadow networks introduce risks of data leakage, unmonitored device connections, and unencrypted communication channels.
Cellular Intrusion Detection (Rogue Femtocell Monitoring)	Without monitoring for rogue femtocells, attackers can deploy fake cellular towers to intercept calls, SMS-based MFA, or data sessions from nearby devices. This allows attackers to capture credentials, perform SIM-based attacks, and monitor sensitive communication without detection.
RFID Anti-Cloning Technology	Lack of anti-cloning controls makes RFID badges susceptible to duplication, allowing unauthorized individuals to gain physical access to restricted areas. Attackers can easily harvest badge data with

	low-cost equipment and create identical copies to bypass security checks.
RFID Access Log Monitoring & Alerting	If access logs are not monitored, unauthorized entry attempts or suspicious badge activity can go unnoticed for long periods. This enables attackers or malicious insiders to move throughout secure areas undetected, increasing risks of theft, tampering, or PHI exposure.
BYOD Compliance Enforcement via MDM	Without strict BYOD enforcement, personal devices may connect to the network while lacking encryption, authentication, patching, or malware protection. These unmanaged devices serve as high-risk entry points for malware infections, data exfiltration, and credential compromise.
Application Whitelisting	If application whitelisting is not implemented, devices can run unauthorized or malicious software that bypasses antivirus detection. This vulnerability allows ransomware, credential stealers, or unapproved apps to compromise patient data or disrupt business operations.
Blocking Unauthorized Wireless Adapters	Without blocking unapproved wireless adapters, users can connect rogue Wi-Fi dongles or cellular modems that bypass network security controls and monitoring. This opens the door for data exfiltration through hidden channels and allows devices to connect to untrusted networks that may be controlled by attackers.

(e) List of potential threats to your company that could exploit vulnerabilities of critical assets

Assets Name	Potential Threats
Access Control Risk Management	
Patient Electronic Health Records (EHR) Database	Ransomware encryption demanding payment. SQL injection extracting patient data. Insider theft for dark web sale. Unpatched vulnerabilities enabling remote access. Phishing compromising admin credentials.
Practice Management Software System	Credential stuffing using breached passwords. Malware corrupting billing data. Former employee unauthorized access. Denial-of-service disrupting operations. Vendor breach affecting all clients.
Digital Imaging Software & Storage	Theft of images for identity fraud. Competitor copying diagnostic techniques. Storage failure causing permanent data loss. Malicious deletion by insider. Ransomware targeting imaging archives.
Backup Systems & Data Recovery	Ransomware encrypting backup files. Physical theft of backup media. Misconfiguration preventing restoration. Offsite facility breach. Media degradation over time.
Server Infrastructure	Advanced persistent threat gaining long-term access. Physical server theft during break-in.

	Hardware failure from power surge. Root-level compromise. DDoS overwhelming capacity.
Workstation Computers (per unit)	Laptop theft with unencrypted data. USB malware spreading through network. Keylogger capturing credentials. Unpatched OS vulnerabilities. Drive-by malware downloads.
Network Equipment (routers, switches, firewalls)	Default password exploitation. Firmware vulnerabilities. DoS flooding. Man-in-the-middle interception. Rogue access points.
Patient Portal System	Brute force password attacks. Session hijacking. Cross-site scripting. Password reset exploitation. Credential stuffing from breaches.
Digital X-Ray Systems (Panoramic & Intraoral X-ray)	Equipment theft during break-ins. Malware infection. Electromagnetic interference. Firmware manipulation. Physical vandalism.
CEREC/CAD-CAM System	$100K+ equipment theft. Design file theft. Malware corrupting designs. Supply chain attack. Competitor sabotage.
Cone Beam CT Scanner (CBCT)	High-value equipment theft. Patient data theft from imaging files. Safety system tampering. Network vulnerabilities. Natural disaster damage.
Dental Operatory Equipment	After-hours vandalism. Employee sabotage. Natural disaster destruction. Power surge damage. Handpiece theft.
Sterilization Equipment	Equipment tampering. Calibration hacking. Documentation falsification. Physical damage. Compliance data manipulation.
Office Building	Burglary accessing medications. Arson or fire. Natural disasters. Unauthorized entry. Vehicle collision damage
Security System (cameras, alarms)	System tampering. Alarm bypass. Footage deletion. Internet outage. False alarm fatigue.
Phone System	Toll fraud. Eavesdropping. Caller ID spoofing. VoIP interception. DoS attacks.
Patient List/Active Patient Base	Employee theft for competing practice. Competitor patient poaching. Marketing breach. Insider selling to brokers. Ransomware hostage.
Reputation & Brand Value	Data breach disclosure. Negative review campaigns. Social media attacks. HIPAA penalties. Malpractice publicity.
Insurance Contracts/Provider Networks	Credentialing theft. Contract detail leaks. Unauthorized access violations. NPI fraud. Network exclusion.
Website & Online Presence	Website defacement. DDoS attacks. SEO manipulation. Malware injection. Domain hijacking.
Professional Licenses (DEA, State Dental License)	DEA number theft. Identity fraud. Fraudulent prescriptions. License suspension. Criminal investigation.

NPI Numbers	Insurance fraud. Unauthorized claims. Medicare fraud investigation. Financial losses. Provider sanctions.
Insurance Credentialing	Portal credential theft. Fraudulent claims. Payment redirection. Claim manipulation. Network removal.
Network Infrastructure Security Risk Management	
Targeted Healthcare Ransomware Campaign	Ransomware spreads from compromised workstation across entire Clinical VLAN, encrypting EHR database, practice management system, digital imaging archives, and backup systems
Cryptomining Malware Installation	Employee downloads fake "imaging enhancement tool" that installs cryptomining malware consuming system resources
Wiper Malware Attack	Destructive malware permanently deletes patient records, financial data, and system configurations
Insider Threat - Malicious Employee Data Theft	Employee facing termination copies patient database to USB drives or personal cloud storage over several weeks before leaving. Without DLP, exports go undetected.
Advanced Persistent Threat (APT) - Silent PHI Exfiltration	sophisticated attackers establish backdoor, slowly exfiltrate patient records over 6-12 months. Small data transfers to foreign IP addresses go undetected without geographic filtering and SIEM correlation.
Business Email Compromise (BEC) with Data Theft	Attackers monitor email for weeks, harvest patient payment information, employee W-2 data, and insurance details. Send fraudulent wire transfer requests to accounting.
Third-Party Vendor Breach (Business Associate)	Compromised vendor credentials used to access BrightSmile Dental Group (Fictional) systems. Lateral movement and data exfiltration occurs through trusted connection.
Router/Firewall Exploitation via Known CVEs	Attacker scans for vulnerable Unified Threat Management (UTM) devices, exploits known CVE to gain administrative access to network core
Network Device Admin Credential Compromise	Stolen credentials used to log into firewall/switch management interface without MFA. Attacker modifies firewall rules, creates backdoors, disables logging, and establishes persistent access.
International Brute Force & Scanning Attacks	Thousands of login attempts daily from countries with zero business justification. Eventually weak password is cracked or zero-day vulnerability exploited.
Firewall Rule Drift & Accidental Exposure	IT support creates broad firewall rule to quickly resolve connectivity issue. Rule never removed. Six months later, attacker discovers exposed management interface or database port accessible from Internet.

Medical Device Ransomware Lock-out	Ransomware encrypts control systems for dental chairs, sterilization equipment, compressors, and digital imaging systems
Digital X-Ray System Compromise	Attacker pivots from compromised workstation to digital X-ray systems, CEREC, or CBCT scanners. These devices often cannot be patched and run legacy operating systems.
Watering Hole Attack via Dental Association Website	Attackers inject malware into trusted dental association website. Employees visiting for CE credits or updates get infected.
Spear Phishing Against Key Personnel	Attacker research practice on social media, sends convincing email appearing from dental association, insurance company, or equipment vendor requesting login to "update billing information"
Distributed Denial of Service (DDoS) Attack	Practice receives extortion email demanding Bitcoin payment. When ignored, DDoS attack makes website, patient portal, and online booking system unavailable for days.
Backup System Encryption/Deletion	Modern ransomware variants seek out and destroy backups before encrypting production systems. Without proper segmentation, both production and backup systems compromised simultaneously.
After-Hours Physical Server Access	Attacker with building access (cleaning crew, former employee with unrevoked key) enters server closet after hours, boots server from USB to bypass OS security, or installs hardware keylogger on server or firewall.
Network Infrastructure Management Security Risk Management	
EHR server, medical imaging devices, patient records, file server	Missing medical device segmentation, lack of DLP monitoring. Phishing emails with malicious attachments infect workstations, then spread laterally to medical devices on same network segment, encrypting all patient data and demanding ransom payment.
Patient database, 10,000+ PHI records, financial information	Missing Data Loss Prevention (DLP), no USB device control. Export entire patient database to USB drive or email to personal account before termination, then sell patient data on dark web or use for competitive advantage.
Email system, business bank accounts, patient data attachments	Missing DLP email monitoring, limited user awareness. Compromise employee email accounts through phishing, then send fraudulent wire transfer requests or exfiltrate patient data attachments to external addresses.
WiFi credentials, network access, VPN authentication	Missing Wireless Intrusion Prevention System (WIPS). Create fake wireless access point in parking lot broadcasting " BrightSmile Dental Group (Fictional) Staff" network, capturing credentials when staff devices automatically connect.

Banking credentials, financial accounts, business passwords	Missing DNSSEC validation, no DNS filtering. DNS responses to redirect users from legitimate banking, vendor, or insurance websites to attacker-controlled phishing sites that steal credentials.
User credentials, financial accounts, patient data, administrative access	Human vulnerabilities, limited user awareness, missing DLP to catch unusual data transfers. Phone calls or emails pretending to be IT support, vendors, or management tricking employees into revealing passwords, transferring money, or installing malware.
Patient database, executive communications, business strategy, financial data	Missing DLP, no host-to-host VPN for sensitive communications, limited activity monitoring. Abuse legitimate access to steal patient data, sabotage systems, eavesdrop on executive communications, or sell confidential information to competitors.
Entire patient database, all financial records, complete network infrastructure	Multiple gaps including uRPF, IP Source Guard, NAC, DLP, DNS filtering, SNMP monitoring. Gain initial access through supply chain compromise, exploit multiple security gaps simultaneously, operate stealthily over months exfiltrating data slowly to avoid detection.
Medical devices, workstations, servers, network infrastructure	Missing medical device segmentation, limited NAC device compliance checking. Infect workstation through compromised website or email, then scan network for vulnerable systems exploiting unpatched medical devices sharing same VLAN.
Database Security Risk Management	
Electronic Health Records (EHR) System	The EHR system is vulnerable to ransomware and data breaches where attackers could encrypt or steal patient records, leading to HIPAA violations and service disruption.
Patient Billing and Insurance Database	This system faces threats from credential theft and business email compromise (BEC), allowing attackers to alter billing data or redirect insurance payments for financial gain.
Practice Management Software (PMS)	The PMS could be targeted by malware or denial-of-service (DoS) attacks that disrupt scheduling and communication, halting daily clinic operations.
Local and Cloud Backup Servers	Backup servers are at risk of tampering or ransomware attacks that encrypt or delete backups, preventing data recovery during incidents.
Corporate Network Infrastructure	The network is susceptible to IP spoofing, VLAN hopping, and other intrusion attacks that could allow unauthorized access or data interception.
Email and Communication Systems	Email platforms are exposed to phishing and social engineering attacks designed to steal credentials or deliver malicious attachments.
Employee Workstations and Laptops	Endpoints can be compromised by malware or keyloggers that capture credentials or exfiltrate sensitive patient and business data.

Clinic Imaging Systems (X-ray, 3D Scanners)	Imaging systems could be exploited through unpatched firmware or network intrusions, leading to loss or corruption of diagnostic images.
Web Portal (Patient Access)	The patient web portal is vulnerable to brute-force login attempts, session hijacking, and injection attacks that expose patient information.
Physical Office Systems (POS Terminals, Front Desk)	Physical and administrative systems face risks from social engineering or device theft, resulting in unauthorized access to patient or payment data.
Applications Development Security Risk Management	
Patient Database (EHR/ePHI)	Ransomware could encrypt sensitive patient data for ransom; insiders may intentionally or accidentally expose data; external attackers may exploit vulnerabilities in the SQL server or weak passwords to exfiltrate records.
Application Server (Dental Management & Scheduling System)	Exploiting insecure web applications could allow attackers to manipulate or steal sensitive data; weak authentication could enable unauthorized administrative access.
File Server (Documents, X-rays, Billing Records)	Malware or system failures may corrupt or delete important files, while lack of proper access control or backups can lead to permanent data loss.
Cloud Backup & Storage	Misconfigured cloud settings or compromised admin credentials could expose or delete backups, while service outages could disrupt recovery operations.
Network Infrastructure (Switches, Firewalls, Routers)	Distributed Denial-of-Service attacks could disrupt clinical operations; outdated firmware or misconfigured firewalls could allow unauthorized access.
Endpoint Devices (Workstations, Laptops)	Employees may fall victim to phishing emails leading to credential theft or malware infections; unauthorized external devices may introduce viruses or leak data.
Medical Devices (X-ray, CAD/CAM Systems)	Internet-connected devices with weak security can be exploited to gain access to the internal network; outdated software increases the risk of exploitation.
Email System & Communication Platforms	Attackers may impersonate staff to steal funds or data, or distribute malware via infected attachments or links.
Wireless Networks (Wi-Fi – Staff & Guest)	Weak Wi-Fi encryption or unauthorized access points can expose internal traffic or allow attackers to bypass VLAN segmentation.
Physical Office Systems (Workstations, Server Room, Backup Drives)	Physical theft of unencrypted devices or tampering with servers could lead to data loss, system downtime, and compliance violations.
Wireless Security Risk Management	
Patient Database (EHR/ePHI)	In a wireless environment, attackers may attempt to intercept unencrypted or weakly protected Wi-Fi traffic to capture PHI transmitted between

	workstations and the database. Additionally, rogue access points or "evil twin" Wi-Fi networks can trick staff into entering credentials, enabling unauthorized access to the patient database.
Application Server (Dental Management & Scheduling System)	If an attacker compromises the wireless network, they can perform man-in-the-middle attacks to intercept or alter communications between staff devices and the application server. Weak Wi-Fi authentication or stolen wireless credentials may also allow unauthorized users to access the internal network and directly target the server.
File Server (Documents, X-rays, Billing Records)	Endpoints connected through insecure wireless networks may be compromised, allowing attackers to move laterally and access the file server. Wireless-based malware infections, such as ransomware can propagate from a compromised device and encrypt or exfiltrate sensitive files stored on the server.
Cloud Backup & Storage	If wireless sessions are not properly secured, attackers can hijack active cloud backup connections, gaining access to stored patient records and configuration files. Fake Wi-Fi hotspots can also capture cloud administrative login credentials, enabling unauthorized manipulation or deletion of cloud backups.
Network Infrastructure (Switches, Firewalls, Routers)	Compromising the wireless network allows attackers to pivot into the network infrastructure and alter configurations, disable protections, or create backdoors. Wireless denial-of-service attacks such as deauthentication floods can disrupt connectivity and degrade firewall and router monitoring.
Endpoint Devices (Workstations, Laptops)	Endpoints connected through insecure or spoofed Wi-Fi networks can be exposed to session hijacking, credential theft, and wireless exploit attacks. Once an endpoint is compromised over Wi-Fi, attackers may gain direct access to internal systems, EHR portals, and administrative tools.
Medical Devices (X-ray, CAD/CAM Systems)	Bluetooth-enabled or wireless-controlled medical devices may be hijacked by attackers in close proximity who exploit weak pairing or outdated firmware. Wireless interference or unauthorized device connections can disrupt imaging, corrupt diagnostic data, or render equipment temporarily unusable.
Email System & Communication Platforms	Wireless phishing attacks using rogue access points can redirect users to fake email login portals, enabling attackers to capture credentials and compromise communication systems. Furthermore, infected wireless devices can introduce malware through email attachments or messaging tools.

Wireless Networks (Wi-Fi – Staff & Guest)	Weak Wi-Fi passwords, poor encryption, or misconfigured access points expose the wireless network to eavesdropping and unauthorized access. If guest and staff networks are not fully segmented, attackers may pivot from the guest network into internal systems through wireless vulnerabilities.
Physical Office Systems (Workstations, Server Room, Backup Drives)	Wireless RFID card cloning or attacks on wireless door systems may allow unauthorized intruders to physically enter sensitive areas such as the server room. Once inside, attackers can steal, tamper with, or destroy on-site equipment and backup drives, resulting in significant operational and data loss.

(f) List of potential risks for critical assets where Cybersecurity Implementation Controls are missing

Missing Cybersecurity Control	Potential Risks
Access Control Risk Management	
Digital Certificates	Patient records may be intercepted during insurance submissions. This allows attackers to steal sensitive medical information without detection.
API Keys/Access Tokens	Unauthorized users can access patient information through unsecured third-party integrations. This creates a direct pathway for data theft and privacy violations.
Domain Account Credentials	Servers are at risk of brute-force attacks when weak credentials are used. A successful attack compromises the entire network.
Vendor/Contractor ID	Vendors using shared credentials can deploy ransomware without accountability. Tracing the attack back to an external technician becomes impossible.
Biometric Authentication	When passwords are shared, it is unclear which employee accessed sensitive records. HIPAA or privacy violations cannot be attributed to a specific individual.
Smart Card/Badge Authentication	Remote servers can be compromised with stolen passwords. Without a physical token, there is no secondary security barrier.
Hardware Security Keys (FIDO Keys)	Phishing campaigns easily steal portal credentials. Attackers can then submit fraudulent insurance claims.
Mobile Push Notifications	Suspicious login attempts go undetected without real-time notifications. Compromised accounts may remain active for months.
Time-Based One-Time Passwords (TOTP)	Credentials remain valid indefinitely when not rotated. Attackers reuse stolen or breached passwords through stuffing and replay attacks.
Certificate-Based Authentication	Stolen passwords grant immediate network access without device checks. There is no assurance that connecting devices are secure or compliant.

Risk-Based/Adaptive Authentication	Systems fail to flag logins from unusual locations or times. Compromised accounts operate freely without additional checks.
Privileged Access Management (PAM)	Shared or permanent admin credentials hide malicious activities. Without monitoring, privilege misuse cannot be traced.
Attribute-Based Access Control (ABAC)	User fatigue from multiple logins leads to password reuse and weak security. Revoking access centrally is difficult and often delayed.
Mandatory Access Control (MAC)	Permissions remain static regardless of context. Temporary or low-level users may retain access far beyond their role.
Single Sign-On (SSO)	All data is treated equally without sensitivity-based enforcement. This exposes financial and clinical information to the same level of risk.
Key Cards/Proximity Cards	Lost or duplicated keys allow unauthorized physical entry. There are no electronic logs for auditing access.
Smart Cards with PIN	Physical credentials alone are insufficient for identity verification. If lost or copied, they grant immediate access.
Mantrap/Airlock Doors	Tailgating and piggybacking allow multiple people into restricted areas. Security checkpoints cannot enforce one-person entry.
Turnstiles and Gates	Multiple individuals may enter with a single credential swipe. Physical enforcement of secure access is absent.
Bollards and Barriers	Buildings remain vulnerable to vehicle-based attacks like ram-raiding. High-value equipment can be stolen within minutes.
Security Guards	Suspicious activity and break-ins may go unnoticed without human monitoring. Delays in response extend the impact of an incident.
Fingerprint Scanners	Passwords can be shared or denied later, leaving no biological proof of identity. This weakens accountability for sensitive operations.
Facial Recognition	Systems cannot verify if the authenticated user remains present. Walk-away sessions may be abused by unauthorized individuals.
Iris Scanning	High-value assets are not protected with the strongest available biometric security. Critical systems remain accessible with weaker credentials.
Retinal Scanning	Ultra-sensitive transactions and medical data are still accessed with basic passwords. Lack of retinal verification undermines non-repudiation.
Voice Recognition	Attackers impersonate users over the phone or spoof caller IDs. Without voice biometrics, verbal authorizations cannot be trusted.
Network Infrastructure Security Risk Management	

EHR Database Ransomware Encryption	Without micro-segmentation, ransomware can spread laterally from any infected workstation on the Clinical VLAN to encrypt the entire EHR database, causing complete operational shutdown
Backup System Encryption During Ransomware	Without proper isolation, modern ransomware variants can locate and encrypt backup systems simultaneously with production data, eliminating recovery options and forcing ransom payment
Silent PHI Exfiltration Over Extended Period	Without DLP, authorized users can systematically export patient records to external devices or personal accounts undetected over weeks/months
Patient List/Database Theft for Competition	Without DLP, disgruntled employees or those recruited by competing practices can export the complete patient database with contact information for competitor solicitation campaigns
Network Core Compromise via Outdated Firmware	Without systematic firmware patching, attackers can exploit published vulnerabilities to gain complete control of network infrastructure, intercepting all traffic including PHI transmissions
Administrative Credential Compromise & Backdoor Creation	Without MFA protecting network device management interfaces, a single successful phishing attack against IT administrator grants attackers complete control to modify firewall rules, disable security controls, and establish persistent backdoors.
Undetected Advanced Persistent Threat (APT)	Without centralized SIEM, sophisticated multi-stage attacks remain undetected for months while attackers slowly exfiltrate PHI and establish persistent backdoors.
Delayed Incident Detection & Response	Without centralized logging, security incidents are detected days or weeks late through user reports rather than automated alerts, allowing attackers extended time to exfiltrate data and establish persistence.
Medical Device Manipulation & Patient Safety Incident	Without proper micro-segmentation, attackers can pivot from compromised workstation to medical imaging devices, potentially manipulating diagnostic images and causing patient misdiagnosis.
Credential Misuse from Unattended Workstation	Without continuous session validation, logged-in workstations left unattended during patient transitions can be accessed by unauthorized individuals (visitors, patients, cleaning staff) to view/modify PHI.
Business Email Compromise (BEC) Financial Fraud	Without continuous authentication and DLP monitoring, attackers who compromise executive email accounts can monitor communications and send convincing fraudulent wire transfer requests or W-2 phishing to accounting staff.
Unauthorized Software Execution & Malware Installation	Without application whitelisting, employees can accidentally execute malicious software disguised as

	legitimate tools (fake updates, trojanized utilities), enabling cryptominers, keyloggers, or backdoors.
Physical Server Room Intrusion & Hardware Tampering	After-hours physical access to server closet allows attackers to boot servers from USB to bypass software security, install hardware keyloggers, or steal hard drives containing PHI.
Network Infrastructure Management Security Risk Management	
Medical imaging devices, EHR server, patient records, diagnostic capability	Ransomware spreads from infected workstation to X-ray machines and imaging equipment on the same network segment, encrypting patient records and diagnostic systems, resulting in 2–4-week inability to provide comprehensive dental care and $200,000-500,000 in recovery costs.
Patient database, Protected Health Information (PHI), practice reputation	Employee with legitimate access exports 10,000+ patient records via email, USB drive, or cloud upload without detection, resulting in mandatory breach notification, $1,000,000-2,000,000 in regulatory fines, class action lawsuits, and complete loss of patient trust.
EHR access, payment processing, insurance verification, business operations	Single internet connection fails causing cloud-based EHR to become inaccessible, preventing staff from opening patient charts or processing payments, resulting in $2,000-5,000 per day revenue loss during 4–48-hour outage and forced patient rescheduling.
User credentials, WiFi network, patient data, remote access systems	Attacker creates fake "Staff WiFi" network capturing employee credentials when they unknowingly connect to evil twin access point, resulting in unauthorized VPN access to patient data, financial systems compromise, and forced credential reset for all staff members.
Workstations, servers, network integrity, patient data	Employees click phishing links that successfully resolve via DNS to newly registered malicious domains, downloading malware that antivirus misses, resulting in ransomware deployment, credential theft, or botnet infection with $150,000-400,000 recovery costs.
Network infrastructure, business continuity, patient care capability	Core switch or firewall hardware failure with no redundant backup causes complete network outage affecting all operations, resulting in multi-day business shutdown, $6,000-15,000 revenue loss, and patient care disruption while waiting for replacement equipment delivery.
Network access, vendor relationships, patient data, system integrity	Dental equipment vendor connects with malware-infected laptop for remote support and non-compliant device is granted network access based on valid credentials alone, resulting in malware spread, backdoor installation, and potential patient data theft.

Patient database, PHI, competitive intelligence	Employee systematically exfiltrates patient records in small batches over 3-6 months using email or USB without detection, accumulating 5,000+ patient records before resignation, resulting in delayed breach discovery and $500,000-1,500,000 in fines and notification costs.
Financial risk transfer, insurance coverage, business viability	Cyber insurance policy renewal denied, or premiums increase 300-500% due to missing required security controls, resulting in uninsured exposure to ransomware attacks and $200,000-500,000 unrecoverable out-of-pocket costs if incident occurs.
Database Security Risk Management	
Electronic Health Records (EHR) System	Risk of data loss or corruption from incomplete replication and weak network segmentation; could result in inaccessible or inconsistent patient data during recovery.
Patient Billing and Insurance Database	Risk of fraudulent access or data manipulation through phishing or credential theft, caused by insufficient employee awareness and weak policy enforcement.
Practice Management Software (PMS)	Risk of system downtime or scheduling disruptions due to malware or denial-of-service attacks, enabled by partial network protections.
Local and Cloud Backup Servers	Risk of incomplete or failed data recovery during incidents because replication and federation controls are partially implemented and backup integrity checks may be inconsistent.
Corporate Network Infrastructure	Risk of unauthorized network access, IP spoofing, or lateral movement of threats due to incomplete Zero-Trust architecture and gaps in network segmentation.
Email and Communication Systems	Risk of credential compromise, phishing success, or malware infection stemming from insufficient user awareness training and weak phishing defenses.
Employee Workstations and Laptops	Risk of endpoint compromise or malware infection from unpatched systems or unsafe practices, due to incomplete enclave protections and limited training.
Clinic Imaging Systems (X-ray, 3D Scanners)	Risk of data corruption or unauthorized access from network-based attacks exploiting weak enclave and network protection controls.
Web Portal (Patient Access)	Risk of credential stuffing, brute-force attacks, or data exposure due to insufficient network segmentation and weak security awareness among staff managing web access.
Physical Office Systems (POS Terminals, Front Desk)	Risk of unauthorized access or device misuse because of weak policy governance and lack of consistent security enforcement.
Applications Development Security Risk Management	

Patient Database (EHR/ePHI)	Exposure of sensitive health records, HIPAA violations, identity theft, and irreversible data loss during ransomware or hardware failure.
Application Server (Dental Management & Scheduling System)	Unauthorized access to patient or scheduling data, system downtime due to malware injection, and compromise of administrative credentials.
File Server (Documents, X-rays, Billing Records)	Corruption or permanent loss of patient records, ransomware encryption with no recovery option, and data manipulation leading to billing errors.
Cloud Backup & Storage	Unauthorized deletion or download of backups, exposure of confidential data to the public internet, and inability to recover from data breaches.
Network Infrastructure (Switches, Firewalls, Routers)	Internal network compromise, lateral movement of attackers, and full system takeover through unpatched vulnerabilities.
Endpoint Devices (Workstations, Laptops)	Malware propagation, keylogging, and unauthorized data transfer leading to insider or external data exfiltration.
Medical Devices (X-ray, CAD/CAM Systems)	Exploitation of outdated medical systems, unauthorized access to patient scans, and disruption of clinical operations.
Email System & Communication Platforms	Successful phishing or Business Email Compromise (BEC), malware infection, and data exfiltration via email.
Wireless Networks (Wi-Fi – Staff & Guest)	Unauthorized network access, eavesdropping on internal traffic, and compromise of connected devices.
Physical Office Systems (Workstations, Server Room, Backup Drives)	Theft or tampering with physical servers, unauthorized removal of patient data, and inability to track insider incidents.
Wireless Security Risk Management	
Patient Database (EHR/ePHI)	The primary risk is unauthorized disclosure of protected health information (PHI) if attackers intercept wireless communications or steal login credentials through rogue Wi-Fi networks. This exposes the clinic to HIPAA violations, legal liability, financial penalties, and loss of patient trust.
Application Server (Dental Management & Scheduling System)	A wireless compromise risks loss of integrity and availability of scheduling and clinical workflow systems, potentially allowing attackers to alter appointments or disrupt operations. This can lead to service delays, corrupted patient charts, and potential shutdown of essential clinical services.
File Server (Documents, X-rays, Billing Records)	The associated risk is mass data compromise or ransomware encryption if attackers gain wireless access and move laterally to the file server. This results in potential loss of critical patient imaging, billing data, and operational files that could cripple daily functions.

Cloud Backup & Storage	Wireless-based credential theft creates the risk of tampering or deletion of cloud backups, leaving the clinic without recoverable data during an incident. This significantly increases the impact of ransomware attacks and could cause permanent loss of patient records.
Network Infrastructure (Switches, Firewalls, Routers)	If attackers use wireless access to breach the network core, the risk is complete network compromise, allowing them to disable controls, reroute traffic, or create persistent backdoors. Such attacks can collapse network availability and expose all connected systems to exploitation.
Endpoint Devices (Workstations, Laptops)	Compromised endpoints pose the risk of credential theft, data exfiltration, and malware infection entering through wireless attack vectors. Once an endpoint is breached, attackers can escalate privileges and gain unrestricted access to internal systems and patient data.
Medical Devices (X-ray, CAD/CAM Systems)	Compromised endpoints pose the risk of credential theft, data exfiltration, and malware infection entering through wireless attack vectors. Once an endpoint is breached, attackers can escalate privileges and gain unrestricted access to internal systems and patient data.
Email System & Communication Platforms	Compromised endpoints pose the risk of credential theft, data exfiltration, and malware infection entering through wireless attack vectors. Once an endpoint is breached, attackers can escalate privileges and gain unrestricted access to internal systems and patient data.
Wireless Networks (Wi-Fi – Staff & Guest)	Compromised endpoints pose the risk of credential theft, data exfiltration, and malware infection entering through wireless attack vectors. Once an endpoint is breached, attackers can escalate privileges and gain unrestricted access to internal systems and patient data.
Physical Office Systems (Workstations, Server Room, Backup Drives)	Compromised endpoints pose the risk of credential theft, data exfiltration, and malware infection entering through wireless attack vectors. Once an endpoint is breached, attackers can escalate privileges and gain unrestricted access to internal systems and patient data.

(g) List of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks (it is not required to write detailed policies) – Risk Prevention Strategy

Access Control Security Risk Management

- **Identification Credentials:**

- **API Key and Access Token Management Policy**: Secures third-party integrations (imaging software, insurance portals, patient communication platforms) by controlling and auditing automated access, preventing unauthorized cloud service access.

- **Personal Authentication:**
- **Time-Based One-Time Password (TOTP) Policy**: Eliminates credential replay attacks by ensuring stolen passwords expire within 30 seconds, preventing attackers from reusing intercepted login credentials days or weeks later.
- **Multi-Factor Authentication (MFA) Policy**: Blocks 99.9% of automated credential stuffing attacks by requiring second factor even when passwords are stolen, particularly critical for remote access to patient records and billing systems.

- **Authorization:**
- **Role-Based Access Control (RBAC) Policy:** Ensures front desk staff cannot access clinical notes, hygienists cannot modify billing, and insurance coordinators cannot alter treatment plans-limiting damage scope if any account is compromised.
- **Attribute-Based Access Control (ABAC) Policy:** Dynamically adjusts permissions based on context (location, time, device), allowing temporary staff appropriate access during their shift without granting permanent permissions.
- **Least Privilege Access Policy:** Minimizes potential damage from compromised accounts by ensuring users have only the minimum permissions needed for their job, preventing lateral movement during breaches.

- **Logical Access Control Methods:**
- **Encryption Standards and Key Management Policy:** Protects patient data both in transit (insurance claims) and at rest (backup drives), renders stolen laptops/backup media useless to thieves, and ensures HIPAA encryption compliance.
- **Network Segmentation Policy:** Isolates patient database servers from public Wi-Fi guests, prevents ransomware from spreading from reception computers to imaging systems, and contains breaches to single network segments.
- **Cloud Access Security Policy:** Controls access to cloud-based scheduling, imaging storage, and patient portals, ensures only corporate-managed devices can reach cloud PHI, and monitors for suspicious cloud activity.

- **Physical Access Control Methods:**
- **Clean Desk and Clear Screen Policy:** Prevents patient records left on desks overnight from being photographed during break-ins, protects against office equipment theft when staff leave workstations unlocked, and prevents PHI exposure to unauthorized visitors.
- **Facility Access Control Policy:** Designates secure zones (server room, medication storage, records room) requiring additional authentication, prevents general staff from accessing high-value areas, and compartmentalizes physical security.

- **Biometric Systems:**

- **Biometric Authentication Implementation Policy:** Eliminates password sharing in clinical environments where gloved hands make typing difficult, creates definitive proof of which clinician accessed patient records, and prevents users from denying their actions.

Network Infrastructure Security Risk Management

- **Implement Network Micro-segmentation**: Deploy separate VLANs for Clinical Systems, Administrative Workstations, Medical Devices, and Server Infrastructure to prevent ransomware from spreading laterally across the entire network.
- **Deploy Host-Based Firewalls** :Enable Windows Firewall on all endpoints with default-deny rules to block SMB/RDP communication between workstations, preventing ransomware propagation.
- **Enhanced Email Security** :Deploy advanced email threat protection with sandboxing and block executable attachments to prevent ransomware delivery via phishing emails.
- **Implement Air-Gapped Backups** :Deploy immutable backup storage and maintain offline backup copies completely disconnected from the network to ensure ransomware cannot encrypt recovery data.
- **Isolated Backup Network Segment**: Create dedicated backup VLAN with unidirectional data flow and firewall rules blocking all inbound connections to protect backup systems from network-based attacks.
- **Database Activity Monitoring**: Deploy real-time monitoring on the EHR database to alert on bulk data exports or unusual query patterns indicating potential data theft.
- **Automated Vulnerability Management**: Deploy vulnerability scanning for all network devices and subscribe to vendor security advisories to identify and patch known vulnerabilities before exploitation.
- **Network Device Hardening**: Disable unnecessary services like HTTP and Telnet, change default passwords, and use only encrypted protocols (SSH, HTTPS) to reduce attack surface.
- **Virtual Patching**: Deploy Intrusion Prevention System signatures and firewall rules to block exploitation attempts against unpatched vulnerabilities until firmware updates can be applied.
- **Multi-Factor Authentication (MFA) Implementation**: Deploy MFA using hardware tokens or authenticator apps for all network device management interfaces to prevent credential theft from enabling access.
- **Privileged Access Management (PAM)**: Implement password vaulting with automatic 90-day rotation and session recording for all administrative access to prevent credential compromise.
- **Role-Based Access Control (RBAC)**: Define granular administrative roles with minimum necessary privileges to limit damage if an administrator account is compromised.
- **Deploy Security Information & Event Management (SIEM)**: Implement enterprise SIEM solution collecting logs from firewalls, servers, workstations, and applications to correlate multi-stage APT attacks across systems.
- **Threat Intelligence Integration**: Subscribe to threat intelligence feeds and integrate known Indicators of Compromise into the SIEM to automatically detect and block APT infrastructure.
- **Network Traffic Analysis**: Deploy Network Detection and Response solution to monitor for beaconing behavior, command-and-control communications, and data exfiltration patterns.

Network Infrastructure Management Security Risk Management

- **Implement Dedicated Medical Device VLAN (IoT VLAN):** Create VLAN 60 exclusively for medical imaging devices separating X-ray machines, CBCT scanners, and digital cameras from workstations to prevent ransomware lateral movement. Configure strict ACLs permitting medical

devices to communicate only with designated imaging workstation on ports 443 and 3389, blocking all internet access and device-to-device communication.

- **Establish Medical Device Security Baseline:** Document all medical devices with manufacturer, model, OS version, and network requirements creating inventory for vulnerability tracking. Monitor baseline communication patterns and alert on any deviations indicating potential compromise or unauthorized usage.
- **Deploy Email Data Loss Prevention Policies:** Implement Microsoft 365 DLP scanning all outbound emails for Social Security numbers, patient identifiers, and sensitive keywords, automatically blocking emails containing PHI sent to personal email addresses. Configure rules quarantining emails with large attachments (>5MB) to personal domains requiring manager approval before delivery.
- **Enable USB Device Control via Group Policy:** Block USB mass storage devices on all workstations through Group Policy while allowing keyboards and mice, preventing data theft via flash drives. Create exception process where IT Administrator can temporarily enable USB for approved business needs with all connection attempts logged.
- **Implement Cloud Application Monitoring:** Monitor uploads to personal cloud storage services (Dropbox, Google Drive personal, OneDrive personal) blocking or alerting on file transfers containing patient data patterns. Allow only approved corporate cloud services (Office 365 OneDrive for Business) with DLP policies enforced.
- **Establish Dual Internet Service Providers:** Contract with two different ISPs using diverse technologies (cable + fiber or cable + 5G) eliminating single point of failure. Configure automatic failover within 30-60 seconds using health monitoring that pings 8.8.8.8 every 10 seconds, failing over after 3 consecutive failures.
- **Implement Link Aggregation (LACP) on Critical Uplinks:** Run dual cables from each access switch to core switch configuring Link Aggregation Control Protocol (802.3ad) for active-active load balancing. Provides immediate failover if one link fails plus increased bandwidth (2Gbps instead of 1Gbps) during normal operations.
- **Deploy Wireless Intrusion Prevention System (WIPS):** Install dedicated wireless IPS sensors monitoring 2.4GHz and 5GHz spectrum across entire office plus 50-foot perimeter detecting rogue access points and evil twin attacks. Configure automatic detection comparing against authorized AP MAC address list, immediately alerting on fake " BrightSmile Dental Group (Fictional) Staff" networks attempting credential theft.
- **Enable Wireless Attack Detection and Countermeasures:** Monitor for deauthentication attacks, handshake capture attempts, and wireless bridging with automatic response. Send deauth frames disconnecting clients from rogue APs and automatically disable switch ports showing rogue AP MAC addresses.
- **Deploy Secure DNS Filtering (Cisco Umbrella):** Replace standard DNS with Cisco Umbrella cloud-based DNS security (208.67.222.222) blocking malicious domains, phishing sites, and newly registered domains at DNS layer before connections establish. Install roaming client on laptops providing protection even when off-network at home or traveling.
- **Enable DNSSEC Validation:** Configure Active Directory DNS server to validate DNSSEC cryptographic signatures on all DNS responses preventing cache poisoning and pharming attacks.

Reject responses failing validation and alert on repeated failures indicating possible DNS attack in progress.

- **Enable IP Source Guard on All Switch Ports:** Configure IP Source Guard validating source IP addresses against DHCP snooping binding table, dropping packets if source IP doesn't match DHCP assignment. Prevents workstations from manually configuring fake IP addresses to bypass inter-VLAN ACLs and security policies.
- **Deploy Enhanced Network Access Control (NAC):** Implement comprehensive NAC performing pre-connection device posture checks verifying antivirus is current, OS patches applied, firewall enabled, and disk encrypted before granting network access. Automatically assign non-compliant devices to Quarantine VLAN 998 with access only to update servers and remediation portal.
- **Implement Enhanced SNMP Monitoring Dashboard:** Deploy LibreNMS or PRTG Network Monitor adding all devices via SNMPv3 with real-time dashboards showing bandwidth utilization, interface status, and device health. Configure alerts for interface down, CPU >80%, memory >90%, and interface errors exceeding thresholds enabling proactive issue detection.
- **Deploy Database Activity Monitoring:** Implement real-time monitoring on EHR database detecting unusual query patterns including mass exports (1,000+ records), after-hours access, and privilege escalation attempts. Generate immediate alerts when employees access abnormal number of patient records (>50/hour) or initiate database dumps outside maintenance windows.

Database Security Risk Management

- **Network Segmentation and Zero-Trust Architecture:** Implement network segmentation to isolate critical systems and prevent lateral movement. Adopt a Zero-Trust model where users and devices must continuously authenticate and be verified before accessing resources.
- **Multi-Factor Authentication (MFA) Enforcement:** Require multi-factor authentication for all system logins, remote connections, and privileged accounts to reduce the risk of credential theft and unauthorized access.
- **Immutable Backup and Recovery Controls:** Maintain automated, encrypted, and immutable backups to ensure resilience against ransomware and data corruption. Conduct regular restoration drills to verify recovery success.
- **Endpoint Hardening and Secure Configuration:** Standardize and secure endpoint configurations using industry benchmarks such as CIS. Enforce disk encryption, disable unused ports, and install endpoint detection and response (EDR) solutions.
- **Security Awareness and Training Program:** Conduct recurring cybersecurity training and phishing simulations to improve employee awareness and reduce human error vulnerabilities.
- **Encrypted Data Replication and Identity Federation:** Use real-time encrypted replication to maintain data availability and integrity. Implement federated identity management for centralized authentication across systems.

- **SIEM and Incident Response Integration:** Deploy a Security Information and Event Management (SIEM) platform to detect, correlate, and respond to security events efficiently.
- **Email Security and Anti-Phishing Controls:** Implement email authentication protocols (DMARC, DKIM, SPF) and advanced filtering to block phishing attempts and malicious attachments.
- **Access Management and Privileged Account Oversight:** Apply Role-Based Access Control (RBAC) to restrict permissions based on job functions. Conduct quarterly access reviews and immediately revoke access for terminated or inactive users.
- **Physical Security and Environmental Controls:** Secure all data centers and IT facilities with controlled access, surveillance, and logging. Implement environmental controls to protect hardware from damage or tampering.
- **Vulnerability and Patch Management:** Regularly scan systems for vulnerabilities and apply patches promptly to address known threats. Maintain a documented patch management log for auditing and compliance.

Applications Development Security Risk Management

- **Application and Web Security:** Secure all web-facing applications with a Web Application Firewall (WAF) and input validation to prevent SQL injection and cross-site scripting. Conduct static and dynamic testing (SAST/DAST) prior to deployment.
- **Remote Access and VPN Hardening:** Implement SSL/IPsec VPN with multi-factor authentication and device compliance checks. Disable split tunneling and enforce session timeouts to safeguard remote connections from unauthorized access.
- **Physical and Facility Security:** Restrict access to server rooms, network closets, and data storage areas using badges or biometric authentication. Install 24/7 surveillance, alarm systems, and visitor logs to physically protect IT assets.
- **Logging, Monitoring, and Auditing:** Centralize system and security logs for real-time analysis and retain them for at least one year. Set up alerts for unusual activities and perform monthly audits to confirm compliance and data integrity.
- **Network Segmentation and Zero-Trust Architecture**: Implement VLAN segmentation to isolate clinical, administrative, and guest networks, preventing unauthorized lateral movement. Adopt a Zero-Trust model that requires continuous authentication and device verification before granting system access.

- **Multi-Factor Authentication (MFA) Enforcement:** Require multi-factor authentication for all logins, remote access, and privileged accounts to block unauthorized access. Establish an access control policy that enforces adaptive MFA for high-risk sessions and administrative users.
- **Immutable Backup and Recovery Controls:** Maintain automated, encrypted, and immutable backups stored in both on-premises and cloud environments to ensure data recovery in case of ransomware attacks. Conduct quarterly recovery drills to validate data restoration and integrity.
- **Endpoint Hardening and Secure Configuration:** Apply secure configuration baselines based on CIS benchmarks for all devices and servers. Enforce disk encryption, disable unnecessary ports, and install Endpoint Detection and Response (EDR) tools to monitor and contain threats.
- **Patch and Vulnerability Management:** Perform weekly vulnerability scans and apply critical updates within seven days of release to minimize exploitation windows. Maintain an asset inventory with clear remediation timelines and automatic patch compliance reporting.
- **Data Encryption and Privacy Controls:** Use AES-256 encryption for data at rest and TLS 1.3 for data in transit to safeguard sensitive patient and billing information. Enforce encryption standards for backups, mobile devices, and removable media under a strict data protection policy.
- **Email Security and Phishing Prevention:** Deploy a secure email gateway that filters spam, malware, and phishing attempts. Implement DMARC, DKIM, and SPF protocols, and train staff to recognize and report suspicious messages.
- **Access Control and Least Privilege Enforcement:** Adopt Role-Based Access Control (RBAC) to ensure users only have the access necessary for their job functions. Conduct quarterly account reviews, disable inactive accounts, and document all administrative privileges.
- **Incident Detection and Response:** Establish centralized logging via a Security Information and Event Management (SIEM) platform for continuous monitoring. Define clear escalation paths, incident classification, and response procedures for rapid threat containment.
- **Security Awareness and Training:** Offer annual cybersecurity and HIPAA compliance training to all employees. Conduct phishing simulations and monthly awareness briefings to bolster user vigilance against social engineering and insider threats.
- **Business Continuity and Disaster Recovery Planning:** Maintain redundancy for all critical systems and define RTO and RPO objectives for recovery efforts. Test disaster recovery and business continuity plans biannually to ensure minimal downtime and data loss.

Wireless Security Risk Management

- **Multi-Factor Authentication (MFA) Enforcement:** MFA requires users to verify their identity using multiple factors, significantly reducing the risk of credential theft-driven attacks. Even if passwords are compromised, unauthorized access to sensitive dental systems is prevented.
- **WPA3 Wi-Fi Security & Strong Passphrase Management**: Upgrading all wireless networks to WPA3 encryption ensures that transmitted data is protected against eavesdropping and brute-force attacks. Regularly rotated, complex passphrases further prevent unauthorized users from accessing the staff network.
- **Network Segmentation (Staff vs. Guest VLANs):** Separating Wi-Fi networks ensures that guest devices cannot reach internal systems containing patient data or billing applications. Segmentation limits the blast radius of a compromised device by preventing lateral movement.
- **Wireless Intrusion Detection & Prevention (WIDS/WIPS):** WIDS/WIPS detects rogue access points, unauthorized Wi-Fi activity, and attempts to spoof or hijack wireless signals. Automated blocking prevents attackers from connecting to or imitating legitimate wireless infrastructure.
- **SSID Hardening (Hidden SSID + Non-Identifiable Names):** Using a generic, non-business-related SSID name prevents attackers from easily identifying the network as belonging to a healthcare provider. Hiding SSIDs reduces drive-by targeting, though it should be paired with other strong controls.
- **Mandatory Device Encryption (Full-Disk Encryption):** Full-disk encryption ensures that if a laptop, workstation, or portable drive is lost or stolen, data remains unreadable without proper authentication. This reduces the likelihood of unauthorized access to ePHI and internal documents.
- **Endpoint Protection Platform (EPP/EDR) Deployment**: Advanced endpoint detection monitors devices in real time for malware, ransomware, and unauthorized changes. Automatic isolation and remediation prevent threats from spreading across the dental office network.
- **Secure Firmware & Patch Management Program:** Regular updates to routers, firewalls, workstations, medical devices, and wireless access points reduce the risk of exploitation through outdated components. Automated patch cycles ensure vulnerabilities are closed quickly.
- **Mobile Device Management (MDM) for BYOD & PEDs**: MDM enforces encryption, screen locks, and app restrictions on staff mobile devices that access work email or Wi-Fi. It prevents data leakage from personal devices and allows remote wipe if a device is lost or compromised.
- **Strong Access Control & Least Privilege Policies:** Users are assigned only the minimum permissions necessary for their job duties, preventing unnecessary exposure of sensitive systems. Role-based access also helps contain insider threats and compromised accounts.
- **Secure Backup & Immutable Cloud Storage:** Immutable backups prevent deletion or alteration of historical copies, protecting dental records from ransomware attacks. Offline or cloud-based redundancy ensures rapid recovery after cyber incidents or device failures.
- **RFID Hardening (Anti-Cloning & Access Logging):** Where proximity badges or RFID door locks are used, anti-cloning protection prevents attackers from duplicating staff badges. Real-time access logs allow rapid detection of unauthorized or after-hours entry attempts.

(h) List of recommended Hardening Response controls and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience (it is not required to write detailed policies) – Risk Response Strategy

Access Control Security Risk Management

- **Identification Credentials:**
- **Digital Certificate Management Policy**: Prevents man-in-the-middle attacks on insurance claim transmissions and patient portal communications by ensuring all parties can verify authentic sources and encrypted connections.

- **Personal Authentication:**
- **Risk-Based Authentication Policy**: Automatically flags suspicious login attempts (foreign countries, unusual hours, new devices) and requires additional verification, detecting compromised accounts within minutes instead of months.

- **Authorization:**
- **Access Control Review and Recertification Policy:** Quarterly reviews catch permission creep, identify orphaned accounts from former employees, and remove unnecessary access rights before they can be exploited.
- **Privileged Account Authorization Policy:** Controls who can perform system-wide changes, install software, or access all patient records, preventing rogue administrators or compromised admin accounts from causing practice-wide disasters.
- **Data Classification and Access Policy:** Labels PHI, financial records, and business data by sensitivity level, ensuring crown designs receive different protection than DEA numbers and patient SSNs, preventing uniform weak protection across all data types.
- **Separation of Duties Policy:** Requires multiple people to approve high-risk transactions like payroll changes or insurance refunds, preventing single insider from committing fraud.

- **Logical Access Control Methods:**
- **Secure File Transfer Policy:** Eliminates unencrypted email attachments containing patient records, ensures encrypted transfer for referrals and insurance documentation, and prevents accidental PHI exposure.
- **Session Management and Timeout Policy:** Automatically logs out idle workstations after 10 minutes in treatment rooms, prevents unauthorized access to walk-away sessions, and meets HIPAA automatic logoff requirements.
- **Account Lockout and Password Policy:** Stops brute-force password guessing after 5 failed attempts, enforces strong passwords (12+ characters, complexity), and prevents weak passwords like "Dental123" or "Summer2024".

- **Physical Access Control Methods:**
- **After-Hours Access and Monitoring Policy:** Logs all evening/weekend entries, requires manager approval for after-hours access, and enables detection of unauthorized access outside business hours when break-ins most commonly occur.
- **Physical Media Handling and Destruction Policy:** Ensures backup tapes, old hard drives, and paper records are destroyed properly before disposal, prevents dumpster diving attacks, and meets HIPAA media destruction requirements.

- **Biometric Systems:**

- **Biometric Data Privacy and Protection Policy:** Protects stored fingerprints/facial templates from theft, ensures biometric data cannot be reverse engineered to recreate actual fingerprints, and complies with biometric privacy laws like BIPA.

Network Infrastructure Security Risk Management

- **Automated Incident Containment**: Deploy EDR with automatic network isolation capability to disconnect infected workstations within seconds of ransomware detection, preventing lateral spread across the network.
- **Multi-Tiered Backup Architecture:** Maintain three independent backup tiers (onsite disk, offsite cloud, offline tape) ensuring at least one copy survives any single attack scenario including ransomware.
- **Rapid Recovery Infrastructure:** Maintain pre-configured gold image workstations and servers with network-based imaging system capable of restoring 50 systems within 4-8 hours using secure baseline images.
- **Breach Detection & Investigation Platform**: Deploy forensic tools (FTK, EnCase) and maintain incident response retainer with specialized cybersecurity firm for rapid breach investigation, scope determination, and evidence preservation.
- **Breach Notification System:** Maintain pre-configured breach notification templates and contact lists for patients, OCR, state attorney general, and media to meet 60-day HIPAA notification requirements.
- **Network Device Failover Architecture:** Maintain warm standby firewall and core switch with automatic failover capability to restore network connectivity within 5 minutes of primary device failure or compromise.
- **Emergency Credential Rotation System:** Deploy automated password rotation capability that can reset all administrative passwords across network infrastructure within 15 minutes upon compromise detection.
- **APT Eradication Procedures:** Maintain documented procedures for complete APT removal including simultaneous credential resets, malware eradication, backdoor removal, and coordinated network rebuild if necessary.
- **Incident Response Retainer:** Maintain 24/7 incident response retainer with cybersecurity firm providing immediate expert assistance (within 2 hours) when internal capabilities are exceeded or overwhelmed.
- **Medical Device Incident Response Plan:** Develop specialized procedures for medical device compromises prioritizing patient safety, including immediate device shutdown protocols and manual operation fallback procedures.
- **Rapid Session Termination:** Deploy capability to immediately terminate all active sessions for specific user account or all sessions system-wide within 60 seconds upon unauthorized access detection.
- **Wire Transfer Reversal Procedures:** Maintain 24/7 banking contact protocols and documented procedures for emergency wire transfer recalls, with bank notification within 30 minutes maximizing fund recovery chances.

- **Automated Malware Remediation:** Configure EDR with automated malware removal and system restoration capabilities, reducing remediation time from hours to minutes with minimal manual intervention.
- **Emergency Hardware Replacement:** Maintain rapid deployment spare hardware inventory (firewall, switch, router, servers) enabling complete infrastructure replacement within 8 hours if physical tampering or hardware failure detected.
- **Business Continuity Operations Center:** Establish alternate work location with pre-configured workstations, internet connectivity, and VoIP phones enabling 20 staff to operate remotely within 4 hours of primary site unavailability.

Network Infrastructure Management Security Risk Management

- **Immediate Network Isolation and Containment:** Immediately disconnect all affected workstations from network by disabling switch ports or physically unplugging Ethernet cables to prevent ransomware from spreading to additional systems and medical devices. Disable WiFi on compromised devices and shut down any servers showing encryption activity, preserving unencrypted systems while containing the outbreak to affected systems only.
- **Ransomware Recovery from Immutable Backups:** Restore encrypted patient data from immutable cloud backups that ransomware cannot delete or encrypt, following documented restoration procedures to recover EHR database and patient files. Verify backup integrity before restoration, restore to clean rebuilt systems (not infected originals), and validate all data accessibility before returning to production operations.
- **Forensic Evidence Preservation and Analysis:** Preserve memory captures and disk images from infected systems before cleanup for forensic investigation to determine attack vector, scope of compromise, and data accessed. Engage third-party forensic firm to analyze malware samples, review logs to establish timeline of events, identify patient records potentially accessed, and provide report for HIPAA breach determination and law enforcement.
- **Breach Assessment and Scope Determination:** Immediately investigate suspected data breach by reviewing audit logs to determine exactly which patient records were accessed, by whom, when, and what data was exfiltrated (names, SSNs, medical histories). Conduct forensic analysis of email logs, USB connection logs, cloud upload logs, and file access logs to establish complete timeline and assess whether breach affects 500+ individuals requiring HHS notification.
- **HIPAA Breach Notification Process:** Execute breach notification procedures within 60-day HIPAA deadline: notify all affected patients via first-class mail explaining what happened, what data was involved, steps being taken, and services offered (credit monitoring). Submit breach report to HHS Office for Civil Rights within 60 days if affecting 500+ patients, notify media if breach affects 500+ in same state/jurisdiction, and document all notification activities for regulatory compliance.
- **Credential Reset and Access Revocation:** Immediately reset passwords for all potentially compromised accounts forcing users to create new credentials meeting complexity requirements before next login. Revoke access for terminated employees or suspected insider threats, disable service accounts not recently used, audit all privileged accounts removing unnecessary permissions, and require MFA re-enrollment for affected users ensuring stolen credentials become immediately useless.

- **Immediate Account Suspension and Investigation:** Suspend user account immediately upon suspicion of insider threat or data theft preventing further unauthorized access while investigation proceeds. Preserve all logs and audit trails showing user's activity history including patient records accessed, files downloaded, emails sent, USB connections, and cloud uploads for evidence collection and potential legal proceedings.
- **Legal and Law Enforcement Coordination:** Engage legal counsel immediately to guide investigation ensuring evidence preservation meets legal standards and advising on law enforcement notification requirements. Contact local FBI field office or Secret Service if theft involves 500+ patient records or financial fraud, providing forensic evidence and cooperating with criminal investigation while maintaining attorney-client privilege.
- **Emergency Failover to Backup Systems:** Activate backup internet connection by manually failing over to secondary ISP if automatic failover doesn't trigger, restoring cloud EHR access within 5-10 minutes. Deploy pre-configured spare switch or firewall from secure storage if primary hardware fails, restoring network operations within 2-4 hours using documented emergency procedures and configuration backups.
- **Downtime Communication and Business Continuity:** Immediately notify all staff of network outage via text message or phone calls explaining situation, estimated restoration time, and temporary procedures (paper charts, manual credit card processing). Contact all scheduled patients for the day explaining situation and offering rescheduling options, prioritizing emergency patients who must be seen regardless of system availability.
- **Immediate Session Termination and Lockout:** Terminate all active sessions for compromised user accounts by killing VPN connections, forcing logout from all workstations, and disabling account in Active Directory. Change password immediately, require MFA re-enrollment before account reactivation, and review all account activity in past 90 days to assess damage from unauthorized access.
- **Access Audit and Privilege Review:** Conduct emergency audit of all systems accessed by compromised account reviewing EHR access logs to determine which patient records viewed, file server logs showing documents opened or downloaded, email logs revealing messages read or forwarded, and administrative logs showing configuration changes made. Notify patients if their specific records were inappropriately accessed and document findings for HIPAA breach assessment determination.
- **Malware Containment and Eradication:** Isolate infected workstation from network via VLAN reassignment to Quarantine VLAN 998, preventing lateral spread while maintaining remote access for cleanup. Run full antivirus/EDR scan with latest signatures, use malware removal tools (Malwarebytes, MSRT), and reimage system from clean backup if infection cannot be fully removed, ensuring complete eradication.
- **Post-Infection Vulnerability Remediation:** Identify how malware infected system by reviewing user's recent activities (websites visited, emails opened, USB devices connected, software installed) and determine root cause. Patch exploited vulnerability immediately across all systems, update antivirus signatures, block malicious domains/IPs at firewall, educate user on avoiding similar attacks, and implement additional controls preventing recurrence.

Database Security Risk Management

- **Incident Containment and Isolation Controls:** Immediately isolate affected systems to prevent malware or unauthorized access from spreading to other network segments. Disable compromised accounts and disconnect impacted devices from the network.
- **Data Recovery and Restoration Controls:** Restore critical data and systems from verified, clean backups following a cyber incident. Prioritize essential services to minimize downtime and ensure continuity of operations.
- **Forensic Investigation and Evidence Preservation:** Preserve digital evidence by capturing system logs, memory dumps, and disk images from compromised systems before remediation. This ensures traceability for investigations and compliance reporting.
- **Communication and Escalation Procedures:** Establish a structured communication plan during incidents to notify internal teams, leadership, and external stakeholders in a controlled and compliant manner.
- **Business Continuity and Failover Controls:** Implement redundant systems and failover mechanisms to maintain availability of critical operations when primary systems fail. Use alternative servers or cloud infrastructure for uninterrupted service.
- **Security Patch and Vulnerability Remediation Controls:** Deploy emergency patches and configuration changes after identifying exploited vulnerabilities during an incident. Ensure critical assets are hardened against recurrence.
- **Threat Intelligence and Monitoring Enhancement:** Integrate external threat intelligence feeds and enhance monitoring tools (SIEM, IDS/IPS) to detect new attack patterns related to the incident.
- **Access Credential Reset and Privilege Review:** Reset all compromised user and service credentials immediately after an incident. Reassess access permissions to ensure least-privilege compliance.
- **Ransomware and Malware Containment Controls:** Quarantine infected systems and remove malicious code using secure cleaning tools or reimaging. Disable network shares and block malicious IPs or domains.
- **Post-Incident Review and Improvement Controls:** Conduct a formal post-incident analysis to identify root causes, response gaps, and control weaknesses. Use findings to update response procedures and employee training.
- **Disaster Recovery and Alternate Site Activation:** Activate disaster recovery plans if primary sites are compromised or inoperable, ensuring critical systems resume at alternate locations.
- **Legal and Regulatory Compliance Controls:** Ensure all incident response actions align with legal and regulatory requirements such as HIPAA, GDPR, or state-level breach notification laws.

Applications Development Security Risk Management

- **Incident Response and Containment Procedures:** Establish a formal incident response plan that defines roles, communication protocols, and escalation paths for security breaches. Conduct regular tabletop exercises to ensure staff can quickly isolate affected systems and stop further damage.
- **Disaster Recovery and Business Continuity Planning:** Create and regularly test a Disaster Recovery (DR) plan with clear Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO). Implement system redundancy and cloud failover mechanisms to keep critical operations running during outages.
- **Security Monitoring and Real-Time Detection:** Set up a centralized SIEM tool for ongoing monitoring and correlation of network, application, and system events. Configure automated alerts for unusual activity, privilege escalations, or data theft attempts.
- **Backup Verification and Rapid Restoration Procedures:** Regularly verify backup integrity through automated checks and quarterly test restores. Keep encrypted, offline, and unchangeable backup copies to enable quick recovery after ransomware or data corruption incidents.
- **Threat Intelligence and Vulnerability Response:** Integrate real-time threat intelligence feeds into monitoring systems to detect and respond to emerging threats. Prioritize vulnerabilities based on risk and patch within designated SLA windows.
- **Access Revocation and Account Recovery Controls:** Use automated workflows to instantly revoke compromised or inactive accounts. Monitor privileged access and require credential resets after suspected credential theft or insider misuse.
- **Endpoint Detection and Response (EDR) Implementation:** Deploy EDR solutions that offer real-time behavioral analysis and automated containment for infected devices. Enable forensic capabilities for post-incident investigation and root cause analysis.
- **Network Isolation and Micro-Segmentation Response:** Configure internal firewalls and VLAN micro-segmentation to limit infection spread and lateral movement. Use predefined containment playbooks to dynamically quarantine affected segments during an incident.
- **Communication and Coordination Plan:** Develop a structured communication plan for notifying staff, IT personnel, and law enforcement in case of data breach. Ensure HIPAA-compliant incident reporting and maintain an outside contact list for cyber insurance and recovery partners.
- **Forensic Investigation and Evidence Preservation:** Set up a process for collecting, preserving, and analyzing digital evidence after an incident. Keep a chain of custody and coordinate with legal counsel to ensure compliance with federal and HIPAA breach laws.
- **Post-Incident Review and Lessons Learned:** Perform a root cause analysis within 72 hours of a major incident to find weaknesses in detection and response. Document findings, update playbooks, and modify controls to prevent recurrence.
- **Third-Party and Vendor Risk Management:** Require vendors with network access to meet equivalent cybersecurity controls and provide annual compliance attestations. Include incident reporting and recovery responsibilities in all vendor contracts.
- **Change Control and Configuration Management:** Follow a formal change management process that requires approval and rollback procedures for system updates. Monitor configuration changes in real time to detect unauthorized modifications or policy violations.

- **User Awareness and Recovery Training:** Offer regular refresher training for staff on how to respond during security incidents, including phishing and device isolation. Conduct breach scenario simulations to reinforce quick and proper recovery actions.
- **Policy Enforcement and Continuous Improvement:** Review all cybersecurity and response policies yearly to reflect new threats, technologies, and regulations. Use audit results and incident data to continually enhance organizational resilience.

Wireless Security Risk Management

- **Incident Response Plan (IRP) & Playbooks:** An established IRP ensures that staff know exactly how to respond when critical assets are compromised, reducing confusion and delay during a cybersecurity event. Pre-built playbooks for ransomware, data breaches, and wireless attacks streamline containment and recovery actions.
- **Security Information & Event Management (SIEM) Monitoring:** SIEM platforms collect, correlate, and alert on suspicious activity across servers, endpoints, and wireless logs. Real-time detection helps the organization contain threats early and reduces the impact on critical assets.
- **Automated Device Isolation (EDR/Network Access Control):** Endpoint Detection & Response (EDR) tools can automatically isolate infected workstations or laptops from the network during an attack. This prevents the spread of malware or lateral movement toward servers containing patient data.
- **Immutable Backups & Rapid Recovery Procedures:** Immutable (write-once) backups prevent attackers from deleting or altering recovery data during a breach or ransomware attack. Regularly tested recovery procedures ensure that systems like EHR, scheduling servers, and file servers can be restored quickly with minimal downtime.
- **Network Segmentation for Incident Containment:** Segmentation limits the spread of an attack by confining compromised devices to isolated network zones. This greatly reduces the impact of ransomware or wireless intrusions on high-value assets such as the EHR database.
- **Rapid Patch & Emergency Vulnerability Response Program:** A structured process for rapid patching during emerging threats (e.g., zero-day vulnerabilities) minimizes exposure for critical assets. Emergency patch cycles ensure essential systems like the application server and medical devices are secured quickly after a threat is identified.
- **Role-Based Access Suspension Procedures:** During a suspected compromise, the ability to quickly disable user accounts and revoke privileged access limits attacker reach. Suspicious credentials can be shut down immediately to protect patient data and internal systems.
- **Ransomware Response Toolkit (Decryption Tools, Network Isolation Scripts):** Having dedicated scripts and tools ready for isolating infected devices and analyzing suspicious files shortens incident response time. These predefined resources help secure critical systems faster and reduce operational impact.
- **Wireless Intrusion Response Protocol:** When rogue APs or Bluetooth attacks are detected, pre-defined wireless shutdown and re-authentication procedures can quickly remove the threat. This protects medical devices, EHR endpoints, and wireless networks from sustained compromise.
- **Cloud Failover & Geo-Redundant Replication:** Cloud-based servers and backups should replicate across multiple geographic regions to ensure uptime even during local failures. This

reduces downtime for EHR systems and ensures patient data remains accessible during regional outages.

- **Disaster Recovery Drills & Simulation Exercises:** Regularly testing the recovery of critical assets through simulated cyberattacks increases readiness and highlights gaps in procedures. These exercises ensure staff can respond effectively during real incidents, reducing long-term operational impact.

8.Applicable Government Regulations and Industry Standards discussed in Class 12

- **ISO/IEC 27002:**ISO 17799 was an international standard providing best-practice guidelines for information security management. It covered security policies, organizational security, asset management, access control, incident response, and compliance. It later evolved into ISO/IEC 27002, which continues to serve as a widely adopted framework for implementing security controls.
- **ISO/IEC 27000 series:** The ISO 27000 family provides a comprehensive framework for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS). Within this series, ISO 27001 outlines the specific requirements that organizations must follow to build and manage an effective ISMS. ISO 27002 complements this by offering best-practice security controls that organizations can implement to protect their information assets. ISO 27000 itself defines the key terminology and foundational concepts used throughout the series. Altogether, the ISO 27000 family helps organizations ensure the confidentiality, integrity, and availability of their information.
- **COBIT (Control Objectives for Information and Related Technologies):** COBIT is a comprehensive IT governance and management framework created by ISACA. It helps organizations align IT goals with business objectives, manage risk, and implement effective internal controls. COBIT provides maturity models, process guidance, and performance metrics to strengthen IT governance and compliance.
- **HIPAA Regulation (Health Insurance Portability and Accountability Act):** HIPAA establishes federal standards for protecting patients' medical information (PHI). It includes the Privacy Rule**,** Security Rule**,** and Breach Notification Rule, requiring covered entities and business associates to safeguard electronic health information, limit disclosures, and report breaches. HIPAA applies to healthcare providers, insurers, and any organization that handles PHI. At BrightSmile Dental Group (Fictional), HIPAA ensures that all patient dental records, treatment histories, X-rays, and billing information are securely stored, accessed, and transmitted. Staff must follow the Privacy Rule to avoid improper sharing of patient information, use secure systems for electronic records, and provide patients with notices of privacy practices. If a data breach occurs (e.g., stolen laptop, unauthorized access), the clinic must follow HIPAA's Breach Notification procedures.

- **PCI DSS (Payment Card Industry Data Security Standard):** PCI DSS is a security standard required for any organization that stores, processes, or transmits credit card data. It includes requirements such as maintaining secure networks, encrypting cardholder data, using strong access controls, monitoring systems, and regularly testing security. Compliance helps reduce fraud, prevent data breaches, and ensure secure payment transactions.
- **NIST Risk Management Framework (NIST RMF):** The NIST RMF provides a structured, step-by-step approach for managing cybersecurity risk within federal agencies and organizations that support them. It includes seven steps: Prepare, Categorize, Select, Implement, Assess, Authorize, and Monitor security controls. The RMF helps organizations continuously identify threats, reduce vulnerabilities, and strengthen system security throughout the lifecycle.

9.Rank asset risks and vulnerability risks for your company across Access Control, Network Infrastructure, Network Infrastructure Management, Database, Applications, and Wireless. For this step, you can create a table with columns or rows Access Control, Network Infrastructure, Network Infrastructure Management, Database, Applications, and Wireless, and in each cell place the top 3 asset risks for each category. Then the same for vulnerability risks. Then you can discuss the top 3 asset risk across all categories and the top 3 vulnerability risks across all categories

Control Type	Top 3 Assets Risk for Control Type
Access Control Security Risk Management	1. Unauthorized access to EHR system due to weak authentication 2. Insider misuse of PHI through excessive privileges 3. Theft/loss of access badges leading to unauthorized entry
Network Infrastructure Security Risk Management	1. Compromise of dental imaging systems through insecure LAN 2. Router misconfiguration exposing internal systems 3. Firewall failure allowing external intrusion
Network Infrastructure Management Security Risk Management	1. Unpatched devices enabling network compromise 2. Mismanagement of ports/protocols exposing services 3. Improper monitoring allowing undetected lateral movement
Database Security Risk Management	1. Unauthorized PHI access in patient database 2. Data corruption due to system failure or malware 3. Lack of encryption exposing data-in-transit and data-at-rest
Applications Development Security Risk Management	1. EHR application vulnerabilities enabling PHI breach 2. Outdated practice-management software exploited by malware

	3. Misconfigured patient portal exposing patient records
Wireless Security Risk Management Implementation	1. Wi-Fi eavesdropping due to weak WPA2 settings 2. Unauthorized device connections to internal Wi-Fi 3. Rogue access point spoofing clinic network

Top 3 Asset Risks Across All Categories	
Access Control Security Risk Management (Unauthorized Access to EHR & PHI Systems)	Because BrightSmile Dental Group (Fictional) handles Protected Health Information (PHI), unauthorized access (either through weak access control or compromised credentials) represents the highest-impact asset risk. A breach directly violates HIPAA and exposes highly sensitive medical data.
Network Infrastructure Security Risk Management (Network Infrastructure Compromise)	If routers, switches, or firewalls are misconfigured or unpatched, attackers can gain full network access. This places all critical systems at risk, including EHR, imaging systems, billing software, and backups.
Database Security Risk Management (Database Breach of Patient Information)	The patient database holds medical histories, images, insurance data, and PII. A breach would result in severe HIPAA penalties, financial damage, and long-term reputational loss for the dental practice.

Control Type	Top 3 Vulnerability Risk for Control Type
Access Control Security Risk Management	1. Weak passwords and lack of MFA 2. No centralized privilege management 3. Missing automatic account lockout policies
Network Infrastructure Security Risk Management	1. Unpatched routers/switches 2. Weak firewall rules allowing unnecessary traffic 3. Lack of network segmentation
Network Infrastructure Management Security Risk Management	1. Excessive open ports (PPS mismanagement) 2. No device monitoring or log review 3. Insecure device management protocols (e.g., Telnet enabled)
Database Security Risk Management	1. Absence of database encryption 2. Shared administrative accounts 3. Lack of backup validation/testing
Applications Development Security Risk Management	1. Outdated software versions 2. Missing secure coding standards 3. Weak session management in web apps
Wireless Security Risk Management Implementation	1. Default SSID/passwords 2. Guest network not isolated 3. No rogue AP detection

Top 3 Vulnerability Risks Across All Categories

Access Control Security Risk Management (Weak Authentication & Lack of Multi-Factor Authentication)	Weak or single-factor authentication significantly increases the risk of unauthorized PHI access especially in a healthcare environment where insider threats and credential compromise are common.
Applications Development Security Risk Management (Unpatched Network and Application Systems)	Missing security updates on routers, switches, practice management software, and EHR systems allow attackers to exploit known vulnerabilities often leading to ransomware attacks in medical practices.
Network Infrastructure Management Security Risk Management (Lack of Network Segmentation)	If imaging systems, front desk computers, guest Wi-Fi, and the EHR database all reside on the same network, one compromised endpoint leads to full-environment compromise.

10.Cybersecurity Workforce Risk Management Implementation

(a). List of Cybersecurity Specialty Areas that exist in your company (see NCWF, Appendix A2)

- Risk Management (RSK)
- Software Development (DEV)
- Technology R&D (TRD)
- Systems Requirements Planning (SRP)
- Test and Evaluation (TST)
- Systems Development (SYS)
- Data Administration (DTA)
- Knowledge Management (KMG)
- Customer Service and Technical Support (STS)
- Network Services (NET)
- Systems Administration (ADM)
- Legal Advice and Advocacy (LGA)
- Training, Education, and Awareness (TEA)
- Strategic Planning and Policy (SPP)
- All-Source Analysis (ASA)
- Program/Project Management (PMA) and Acquisition
- Cybersecurity Defense Analysis (CDA)
- Cybersecurity Defense Infrastructure Support (INF)
- Incident Response (CIR)
- Vulnerability Assessment and Management (VAM)
- Threat Analysis (TWA)
- Exploitation Analysis (EXP)
- Targets (TGT)
- Collection Operations (CLO)
- Cyber Operations (OPS)
- Digital Forensics (FOR)

(b). List of Cybersecurity Work Roles that exist in your company (see NCWF, Appendix A3)

- Authorizing Official/Designating Representative
- Security Control Assessor
- Secure Software Assessor
- Research & Development Specialist
- Systems Requirements Planner
- System Testing and Evaluation Specialist
- Information Systems Security Developer
- Database Administrator
- Knowledge Manager
- Technical Support Specialist
- Network Operations Specialist
- System Administrator
- Cyber Defense Analyst
- Cyber Defense Infrastructure Support Specialist
- Cyber Defense Incident Responder
- Vulnerability Assessment Analyst

(c). List of Cybersecurity Tasks that exist in your company (see NCWF, Appendix A4)

Task ID	Task Description
T0001	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.
T0008	Analyze and plan for anticipated changes in data capacity requirements.
T0009	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.
T0010	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
T0011	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.
T0012	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.
T0013	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.
T0014	Apply secure code documentation.
T0015	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.
T0016	Apply security policies to meet security objectives of the system.

T0017	Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.
T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.
T0033	Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.
T0035	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).
T0039	Consult with customers to evaluate functional requirements.
T0041	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.
T0045	Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions.
T0047	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
T0050	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
T0051	Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.
T0052	Define project scope and objectives based on customer requirements.
T0062	Develop and document requirements, capabilities, and constraints for design procedures and processes.
T0065	Develop and implement network backup and recovery procedures.
T0071	Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).
T0081	Diagnose network connectivity problem.
T0082	Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.
T0084	Employ secure configuration management processes.
T0085	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.
T0086	Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.
T0088	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.
T0089	Ensure that security improvement actions are evaluated, validated, and implemented as required.
T0090	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.
T0095	Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy.

T0099	Evaluate cost/benefit, economic, and risk analysis in decision-making process.
T0108	Identify and prioritize critical business functions in collaboration with organizational stakeholders.
T0121	Implement new system design procedures, test procedures, and quality standards.
T0123	Implement specific cybersecurity countermeasures for systems and/or applications.
T0125	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
T0126	Install or replace network hubs, routers, and switches.
T0127	Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements.
T0128	Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.
T0129	Integrate new systems into existing network architecture.
T0137	Maintain database management systems software.
T0139	Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.
T0140	Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.
T0146	Manage the compilation, cataloging, caching, distribution, and retrieval of data.
T0152	Monitor and maintain databases to ensure optimal performance.
T0153	Monitor network capacity and performance.
T0156	Oversee and make recommendations regarding configuration management.
T0160	Patch network vulnerabilities to ensure that information is safeguarded against outside parties.
T0161	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
T0162	Perform backup and recovery of databases to ensure data integrity.
T0163	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
T0163	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
T0164	Perform cyber defense trend analysis and reporting.
T0169	Perform cybersecurity testing of developed applications and/or systems.
T0170	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
T0175	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
T0177	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
T0182	Perform tier 1, 2, and 3 malware analysis.
T0187	Plan and recommend modifications or adjustments based on exercise results or system environment.
T0190	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).

T0194	Properly document all systems security implementation, operations, and maintenance activities and update as necessary.
T0196	Provide advice on project costs, design concepts, or design changes.
T0200	Provide feedback on network requirements, including network architecture and infrastructure.
T0202	Provide cybersecurity guidance to leadership.
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
T0210	Provide recommendations on new database technologies and architectures.
T0212	Provide technical assistance on digital evidence matters to appropriate personnel.
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
T0215	Recognize a possible security violation and take appropriate action to report the incident, as required.
T0216	Recognize and accurately report forensic artifacts indicative of a particular operating system.
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
T0230	Support the design and execution of exercise scenarios.
T0232	Test and maintain network infrastructure including software and hardware devices.
T0238	Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).
T0240	Capture and analyze network traffic associated with malicious activities using network monitoring tools.
T0241	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.
T0243	Verify and update security documentation reflecting the application/system security design features.
T0247	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.
T0248	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
T0249	Research current technology to understand capabilities of required system or network.
T0253	Conduct cursory binary analysis.
T0279	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
T0285	Perform virus scanning on digital media.
T0286	Perform file system forensic analysis.
T0287	Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).
T0288	Perform static malware analysis.
T0289	Utilize deployable forensics toolkit to support operations as necessary.
T0294	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).
T0295	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
T0296	Isolate and remove malware.

T0297	Identify applications and operating systems of a network device based on network traffic.
T0298	Reconstruct a malicious attack or activity based off network traffic.
T0299	Identify network mapping and operating system (OS) fingerprinting activities.
T0305	Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.
T0306	Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.
T0307	Analyze candidate architectures, allocate security services, and select security mechanisms.
T0309	Assess the effectiveness of security controls.
T0310	Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.
T0312	Coordinate with intelligence analysts to correlate threat assessment data.
T0330	Maintain assured message delivery systems.
T0332	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.
T0344	Assess all the configuration management (change configuration/release management) processes.
T0345	Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.
T0352	Conduct learning needs assessments and identify requirements.
T0357	Create interactive learning exercises to create an effective learning environment.
T0365	Develop or assist in the development of training policies and protocols for cyber training.
T0367	Develop the goals and objectives for cyber curriculum.
T0380	Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers.
T0396	Process image with appropriate tools depending on analyst’s goals.
T0397	Perform Windows registry analysis.
T0437	Correlate training and learning to business or mission requirements.
T0454	Define baseline security requirements in accordance with applicable guidelines.
T0463	Develop cost estimates for new or modified system(s).
T0469	Analyze and report organizational security posture trends.
T0470	Analyze and report system security posture trends.
T0475	Assess adequate access controls based on principles of least privilege and need-to-know.
T0497	Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.
T0503	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.
T0504	Assess and monitor cybersecurity related to system implementation and testing practices.

T0526	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
T0545	Work with stakeholders to resolve computer security incidents and vulnerability compliance.
T0548	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.
T0563	Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.
T0569	Answer requests for information.
T0575	Coordinate for intelligence support to operational planning activities.
T0576	Assess all-source intelligence and recommend targets to support cyber operation objectives.
T0579	Assess target vulnerabilities and/or operational capabilities to determine course of action.
T0581	Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.
T0583	Provide subject matter expertise to the development of a common operational picture.
T0584	Maintain a common intelligence picture.
T0585	Provide subject matter expertise to the development of cyber operations specific indicators.
T0586	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.
T0587	Assist in the development and refinement of priority information requirements.
T0589	Assist in the identification of intelligence collection shortfalls.
T0590	Enable synchronization of intelligence support plans across partner organizations as required.
T0592	Provide input to the identification of cyber-related success criteria.
T0593	Brief threat and/or target current situations.
T0597	Collaborate with intelligence analysts/targeting organizations involved in related areas.
T0615	Conduct in-depth research and analysis.
T0617	Conduct nodal analysis.
T0660	Develop information requirements necessary for answering priority information requests.
T0685	Evaluate threat decision-making processes.
T0687	Identify threats to Blue Force vulnerabilities.
T0862	Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.
T0863	Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.
T0863	Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.
T0864	Liaise with regulatory and accrediting bodies.
T0865	Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.

T0866	Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.
T0867	Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.
T0975	Work with the organizational risk analysts to ensure risk metrics are defining realistically to support continuous monitoring.
T0976	Work with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels.
T0977	Establish triggers for unacceptable risk thresholds for continuous monitoring data.
T0978	Work with organizational officials to establish system level reporting categories that can be used by the organization's continuous monitoring program.
T0980	Designate a qualified person to be responsible for the management and implementation of the continuous monitoring program.
T1004	Use continuous monitoring tools to assess risk on an ongoing basis.
T1005	Use the continuous monitoring data to make information security investment decisions to address persistent issues.
T1006	Respond to issues flagged during continuous monitoring, escalate and coordinate a response.
T1007	Review findings from the continuous monitoring program and mitigate risks on a timely basis.

(d). Comparison of the NCWF recommended Cybersecurity Specialty Areas with your company's existing Cybersecurity Specialty Areas

Cybersecurity Specialty Areas	Present/Absent
Risk Management (RSK)	Present
Software Development (DEV)	Absent
Technology R&D (TRD)	Absent
Systems Requirements Planning (SRP)	Present
Test and Evaluation (TST)	Present
Systems Development (SYS)	Present
Data Administration (DTA)	Present
Knowledge Management (KMG)	Present
Customer Service and Technical Support (STS)	Present
Network Services (NET)	Present
Systems Administration (ADM)	Present
Legal Advice and Advocacy (LGA)	Absent
Training, Education, and Awareness (TEA)	Present
Strategic Planning and Policy (SPP)	Present
Program/Project Management (PMA) and Acquisition	Present
Cybersecurity Defense Analysis (CDA)	Present
Cybersecurity Defense Infrastructure Support (INF)	Present
Incident Response (CIR)	Present
Vulnerability Assessment and Management (VAM)	Present
Threat Analysis (TWA)	Absent
Exploitation Analysis (EXP)	Absent

All-Source Analysis (ASA)	Present
Targets (TGT)	Absent
Collection Operations (CLO)	Absent
Cyber Operations (OPS)	Absent
Digital Forensics (FOR)	Absent

(e.) Comparison of the NCWF recommended Cybersecurity Work Roles with your company's existing Cybersecurity Work Roles

Work Roles	Present/Absent
Cyber Instructional Curriculum Developer	Absent
Cyber Instructor	Absent
Information Systems Security Manager	Absent
Communications Security (COMSEC) Manager	Absent
Cyber Workforce Developer and Manager	Absent
Cyber Policy and Strategy Planner	Absent
Executive Cyber Leadership	Absent
Program Manager	Absent
IT Project Manager	Absent
Product Support Manager	Absent
IT Investment/Portfolio Manager	Absent
IT Program Auditor	Absent
Cyber Instructional Curriculum Developer	Absent
Threat/Warning Analyst	Absent
Exploitation Analyst	Absent
All-Source Analyst	Absent
Mission Assessment Specialist	Absent
Target Developer	Absent
Target Network Analyst	Absent
Multi-Disciplined Language Analyst	Absent
All Source-Collection Manager	Absent
All Source-Collection Requirements Manager	Absent
Cyber Intel Planner	Absent
Cyber Ops Planner	Absent
Partner Integration Planner	Absent
Cyber Operator	Absent
All Source-Collection Manager	Absent
All Source-Collection Requirements Manager	Absent
Cyber Intel Planner	Absent
Cyber Ops Planner	Absent
Partner Integration Planner	Absent
Cyber Crime Investigator	Absent
Law Enforcement /Counterintelligence Forensics Analyst	Absent
Cyber Defense Forensics Analyst	Absent

(f). Comparison the NCWF recommended Cybersecurity Tasks with your company's existing Cybersecurity Tasks

Task ID	Task Description	Present/Absent

T0018	Assess the effectiveness of cybersecurity measures utilized by system(s).	Absent
T0019	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	Absent
T0020	Develop content for cyber defense tools.	Absent
T0021	Build, test, and modify product prototypes using working models or theoretical models.	Absent
T0022	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	Absent
T0023	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Absent
T0024	Collect and maintain data needed to meet system cybersecurity reporting.	Absent
T0026	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.	Absent
T0027	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.	Absent
T0028	Conduct and/or support authorized penetration testing on enterprise network assets.	Absent
T0029	Conduct functional and connectivity testing to ensure continuing operability.	Absent
T0030	Conduct interactive training exercises to create an effective learning environment.	Absent
T0031	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.	Absent
T0032	Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Absent
T0046	Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.	Absent
T0047	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.	Absent
T0048	Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.	Absent
T0049	Decrypt seized data using technical means.	Absent

T0050	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Absent
T0051	Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	Absent
T0100	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Absent
T0101	Evaluate the effectiveness and comprehensiveness of existing training programs.	Absent
T0102	Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.	Absent
T0103	Examine recovered data for information of relevance to the issue at hand.	Absent
T0104	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.	Absent
T0105	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.	Absent
T0106	Identify alternative information security strategies to address organizational security objective.	Absent
T0107	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find workarounds for communication protocols that are not interoperable).	Absent
T0108	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Absent
T0313	Design and document quality standards.	Absent
T0314	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Absent
T0315	Develop and deliver technical training to educate others or meet customer needs.	Absent
T0316	Develop or assist in the development of computer based training modules or classes.	Absent
T0317	Develop or assist in the development of course assignments.	Absent
T0318	Develop or assist in the development of course evaluations.	Absent
T0319	Develop or assist in the development of grading and proficiency standards.	Absent
T0320	Assist in the development of individual/collective development, training, and/or remediation plans.	Absent

T0321	Develop or assist in the development of learning objectives and goals.	Absent
T0322	Develop or assist in the development of on-the-job training materials or programs.	Absent
T0323	Develop or assist in the development of written tests for measuring and assessing learner proficiency.	Absent
T0324	Direct software programming and development of documentation.	Absent
T0325	Document a system's purpose and preliminary system security concept of operations.	Absent
T0326	Employ configuration management processes.	Absent
T0327	Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.	Absent
T0328	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	Absent
T0329	Follow software and systems engineering life cycle standards and processes.	Absent
T0687	Identify threats to Blue Force vulnerabilities.	Absent
T0688	Evaluate available capabilities against desired effects to recommend efficient solutions.	Absent
T0689	Evaluate extent to which collected information and/or produced intelligence satisfy information requests.	Absent
T0690	Evaluate intelligence estimates to support the planning cycle.	Absent
T0691	Evaluate the conditions that affect employment of available cyber intelligence capabilities.	Absent
T0692	Generate and evaluate the effectiveness of network analysis strategies.	Absent
T0693	Evaluate extent to which collection operations are synchronized with operational requirements.	Absent
T0694	Evaluate the effectiveness of collection operations against the collection plan.	Absent
T0695	Examine intercept-related metadata and content with an understanding of targeting significance.	Absent
T0696	Exploit network devices, security devices, and/or terminals or environments using various methods or tools.	Absent
T0697	Facilitate access enabling by physical and/or wireless means.	Absent
T0698	Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers.	Absent
T0699	Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.	Absent
T0700	Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community.	Absent

T0701	Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development.	Absent
T0702	Formulate collection strategies based on knowledge of available intelligence discipline capabilities and gathering methods that align multi-discipline collection capabilities and accesses with targets and their observables.	Absent
T0703	Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities.	Absent
T0704	Incorporate cyber operations and communications security support plans into organization objectives.	Absent
T0705	Incorporate intelligence and counterintelligence to support plan development.	Absent
T0706	Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)	Absent
T0707	Generate requests for information.	Absent
T0708	Identify threat tactics, and methodologies.	Absent
T0709	Identify all available partner intelligence capabilities and limitations supporting cyber operations.	Absent
T0710	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Absent
T0711	Identify, draft, evaluate, and prioritize relevant intelligence or information requirements.	Absent
T0712	Identify and manage security cooperation priorities with external partners.	Absent
T0713	Identify and submit intelligence requirements for the purposes of designating priority information requirements.	Absent
T0714	Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.	Absent
T0715	Identify collection gaps and potential collection strategies against targets.	Absent
T0716	Identify coordination requirements and procedures with designated collection authorities.	Absent
T0717	Identify critical target elements.	Absent
T0718	Identify intelligence gaps and shortfalls.	Absent
T0719	Identify cyber intelligence gaps and shortfalls for cyber operational planning.	Absent
T0720	Identify gaps in our understanding of target technology and developing innovative collection approaches.	Absent
T0721	Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness.	Absent
T0722	Identify network components and their functionality to enable analysis and target development.	Absent

T0723	Identify potential collection disciplines for application against priority information requirements.	Absent
T0724	Identify potential points of strength and vulnerability within a network.	Absent
T0725	Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.	Absent
T0726	Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production.	Absent
T0727	Identify, locate, and track targets via geospatial analysis techniques.	Absent
T0728	Provide input to or develop courses of action based on threat factors.	Absent
T0729	Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities.	Absent
T0730	Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures.	Absent
T0731	Initiate requests to guide tasking and assist with collection management.	Absent
T0732	Integrate cyber planning/targeting efforts with other organizations.	Absent
T0733	Interpret environment preparations assessments to determine a course of action.	Absent
T0734	Issue requests for information.	Absent
T0735	Lead and coordinate intelligence support to operational planning.	Absent
T0736	Lead or enable exploitation operations in support of organization objectives and target requirements.	Absent
T0737	Link priority collection requirements to optimal assets and resources.	Absent
T0738	Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.	Absent
T0739	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Absent
T0740	Maintain situational awareness and functionality of organic operational infrastructure.	Absent
T0741	Maintain situational awareness of cyber-related intelligence requirements and associated tasking.	Absent
T0742	Maintain situational awareness of partner capabilities and activities.	Absent
T0743	Maintain situational awareness to determine if changes to the operating environment require review of the plan.	Absent
T0744	Maintain target lists (i.e., RTL, JTL, CTL, etc.).	Absent
T0745	Make recommendations to guide collection in support of customer requirements.	Absent
T0746	Modify collection requirements as necessary.	Absent

T0747	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	Absent
T0748	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Absent
T0749	Monitor and report on validated threat activities.	Absent
T0750	Monitor completion of reallocated collection efforts.	Absent
T0751	Monitor open-source websites for hostile content directed towards organizational or partner interests.	Absent
T0752	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Absent
T0753	Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture.	Absent
T0754	Monitor target networks to provide indications and warning of target communications changes or processing failures.	Absent
T0755	Monitor the operational environment for potential factors and risks to the collection operation management process.	Absent
T0756	Operate and maintain automated systems for gaining and maintaining access to target systems.	Absent
T0757	Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence requirements.	Absent
T0758	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Absent
T0759	Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.	Absent
T0760	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	Absent
T0761	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
T0762	**WITHDRAWN:** Provide subject matter expertise in course of action development.	Absent
T0763	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Absent
T0764	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	Absent
T0765	Provide subject matter expertise to development of exercises.	Absent
T0766	Propose policy which governs interactions with external coordination groups.	Absent
T0767	Perform content and/or metadata analysis to meet organization objectives.	Absent

T0768	Conduct cyber activities to degrade/remove information resident in computers and computer networks.	Absent
T0769	Perform targeting automation activities.	Absent
T0770	Characterize websites.	Absent
T0771	Provide subject matter expertise to website characterizations.	Absent
T0772	Prepare for and provide subject matter expertise to exercises.	Absent
T0773	Prioritize collection requirements for collection platforms based on platform capabilities.	Absent
T0774	Process exfiltrated data for analysis and/or dissemination to customers.	Absent
T0775	Produce network reconstructions.	Absent
T0776	Produce target system analysis products.	Absent
T0777	Profile network or system administrators and their activities.	Absent
T0778	Profile targets and their activities.	Absent
T0779	Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations.	Absent
T0780	Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.	Absent
T0781	Provide aim point and reengagement recommendations.	Absent
T0782	Provide analyses and support for effectiveness assessment.	Absent
T0783	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Absent
T0784	Provide cyber focused guidance and advice on intelligence support plan inputs.	Absent
T0785	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Absent
T0786	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Absent
T0787	Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	Absent
T0788	Provide input and assist in post-action effectiveness assessments.	Absent
T0789	Provide input and assist in the development of plans and guidance.	Absent
T0790	Provide input for targeting effectiveness assessments for leadership acceptance.	Absent
T0791	Provide input to the administrative and logistical elements of an operational support plan.	Absent

T0792	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	Absent
T0793	Provide effectiveness support to designated exercises, and/or time sensitive operations.	Absent
T0794	Provide operations and reengagement recommendations.	Absent
T0795	Provide planning support between internal and external partners.	Absent
T0796	Provide real-time actionable geolocation information.	Absent
T0797	Provide target recommendations which meet leadership objectives.	Absent
T0798	Provide targeting products and targeting support as designated.	Absent
T0799	Provide time sensitive targeting support.	Absent
T0800	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	Absent
T0801	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	Absent
T0802	Review appropriate information sources to determine validity and relevance of information gathered.	Absent
T0803	Reconstruct networks in diagram or report format.	Absent
T0804	Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.	Absent
T0805	Report intelligence-derived significant network events and intrusions.	Absent
T0806	Request discipline-specific processing, exploitation, and disseminate information collected using discipline's collection assets and resources in accordance with approved guidance and/or procedures.	Absent
T0807	Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.	Absent
T0808	Review and comprehend organizational leadership objectives and guidance for planning.	Absent
T0809	Review capabilities of allocated collection assets.	Absent

(g). List of potential threats to your company that could exploit vulnerabilities of critical assets due to missing Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks

- **Unauthorized Access to EHR/PHI Systems (External Hackers or Insider Threats):** Attackers exploit weak authentication, lack of access-control management, and insufficient monitoring to gain access to patient records.
- **Ransomware Attacks on EHR, Billing, or Imaging Servers:** Cybercriminals leverage missing patch management, absent malware monitoring roles, and outdated systems to encrypt patient data.
- **Data Exfiltration via Email or Cloud Services:** Employees or attackers can send PHI outside the network because there is no DLP analyst, email-security monitoring, or audit logging.

- **Network Intrusion via Misconfigured Firewalls and Routers:** Threat actors penetrate the internal network due to a shortage of network-security engineers managing firewall rules, ACLs, VLAN segmentation, or remote access controls.
- **Wi-Fi Compromise (Rogue Access Points, Cracking Weak WPA Keys): Attackers** exploit weak wireless configurations, default passwords, and the absence of wireless-security administrators.
- **Insider Misuse of Patient Records:** Employees intentionally view, copy, or modify PHI because missing audit-review and monitoring roles allow unauthorized access to go undetected.
- **Compromise of Digital Imaging/X-Ray/PACS Systems:** Attackers manipulate or steal diagnostic images because there is no imaging-system security specialist managing updates, segmentation, or access controls.
- **Billing Fraud or Unauthorized Financial Transactions:** Attackers or insiders exploit inadequate logging, lack of separation-of-duties enforcement, and missing auditing roles to alter billing or insurance submissions.
- **Social Engineering and Phishing Attacks:** Without a cybersecurity awareness trainer or phishing-resilience program, staff are vulnerable to credential-harvesting emails and malicious links.
- **Device Theft Leading to PHI Exposure:** Stolen laptops, tablets, or workstations become data-exposure points due to missing endpoint-security management (device encryption, remote wipe, access logs).
- **Supply-Chain or Vendor Attacks:** Third-party software (EHR vendor, imaging vendor, payment processor) becomes an entry point because there is no vendor-risk-management role in place.
- **Service Outages or Data Loss Due to Failed Backups:** Threat actors exploit the lack of disaster-recovery planning, backup testing, and continuity-of-operations specialists, resulting in long downtime and permanent PHI loss.

(h). List of potential risks for critical assets where Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks are missing

- **Unauthorized access to Electronic Health Records (EHR):** Without access control administrators and IAM specialists, employees may receive excessive privileges, and weak authentication could allow attackers to access or modify patient PHI.
- **Exposure or theft of Protected Health Information (PHI):** Missing privacy/security roles (HIPAA Security Officer, DLP Analyst) increase the risk that PHI is leaked through email, USB devices, or misconfigured patient portals.
- **Ransomware infection on EHR, imaging systems, or billing systems:** Without a cybersecurity operations analyst or patch management specialist, outdated devices and unpatched applications become easy entry points for ransomware.
- **Manipulation or loss of digital imaging (X-ray, PACS) data:** No imaging system security role means imaging servers may be misconfigured, exposing them to corruption, deletion, or unauthorized modification.
- **Fraudulent billing, insurance manipulation, or unauthorized financial access:** Missing auditing and monitoring roles enable attackers or insiders to exploit practice-management or billing systems without detection.

- **Network compromise due to misconfigured firewalls, routers, or VLANs:** Without a network security engineer, the practice could suffer intrusion, lateral movement, or unauthorized connections to dental devices or front-desk systems.
- **Unauthorized access through weak Wi-Fi security:** Absence of wireless security roles results in default passwords, shared SSIDs, improper segmentation between guest Wi-Fi and clinical systems, and higher risk of intrusion.
- **Downtime and data loss from failed backups:** Missing continuity and disaster recovery specialists increase the risk that backups are not tested properly, causing the practice to permanently lose patient records after an outage.
- **Data breaches caused by improper device handling (laptops, workstations, tablets):** No endpoint security or device management roles mean devices may lack encryption, remote wipe capability, or access logging exposing PHI if stolen.
- **Patient portal account takeover:** Without web application security roles, unsecured login mechanisms, weak session controls, and missing MFA allow attackers to access patient histories and appointment data.
- **Insider misuse of patient data:** No monitoring or audit review roles mean unauthorized browsing of patient information; a major HIPAA violation goes undetected.
- **Public reputation damage due to any security incident**: Missing incident response and communication security roles leave the practice unprepared to handle breaches, resulting in prolonged outages, regulatory penalties, and loss of patient trust.

(i). List of recommended policies (Hiring new Cybersecurity staff, educating current staff, outsourcing) for each recommended Cybersecurity Specialty Area, Cybersecurity Work Role, or Cybersecurity Task that should be created to mitigate the identified risks (it is not required to write detailed policies)

- **Risk Management (RSK) / Authorizing Official:** Hire or designate a Risk Management Lead to conduct formal risk assessments, prioritize threats to PHI, and approve security decisions. Provide annual training on HIPAA Security Rule risk analysis.
- **Software Development (DEV) / Secure Software Assessor:** Outsource secure code review for dental practice applications (patient portal, billing). Perform annual third-party application security assessments and train staff on identifying insecure apps.
- **Systems Requirements Planning (SRP) / Systems Requirements Planner:** Assign or contract a planner to ensure new systems (imaging, EHR updates) include HIPAA-aligned security requirements. Train managers on documenting security needs before system acquisition.
- **Systems Development (SYS) / Information Systems Security Developer:** Outsource system customization and secure configuration changes to certified developers. Require annual secure configuration training for internal IT staff.
- **Data Administration (DTA) / Database Administrator:** Hire or outsource a database administrator to manage encryption, backups, and access controls on the EHR database. Train staff on proper PHI handling and minimum-necessary access.
- **Knowledge Management (KMG) / Knowledge Manager:** Designate a Knowledge Manager to maintain secure documentation, control PHI-related knowledge bases, and enforce document access policies. Train employees in secure documentation practices.

- **Customer Service & Technical Support (STS) / Technical Support Specialist:** Provide training to technical support staff on secure troubleshooting, remote access restrictions, and PHI protection. Outsource advanced support for EHR security issues.
- **Network Services (NET) / Network Operations Specialist:** Hire or outsource a network specialist to manage firewalls, router settings, wireless segmentation, and intrusion detection. Train staff on safe network usage and reporting suspicious activity.
- **Systems Administration (ADM) / System Administrator:** Hire or train a system administrator to perform patching, endpoint hardening, device encryption, and access management. Establish mandatory quarterly security configuration checkups.
- **Cybersecurity Defense Analysis (CDA) / Cyber Defense Analyst:** Outsource real-time monitoring (SIEM/MSSP) to detect malicious activity, while training internal staff on recognizing signs of compromise.
- **Incident Response (CIR) / Incident Responder:** Hire or contract an incident responder and develop an IR plan. Conduct biannual tabletop exercises to train staff on reporting and responding to ransomware, PHI breaches, and system outages.
- **Vulnerability Assessment & Management (VAM) / Vulnerability Assessment Analyst:** Outsource regular vulnerability scans and penetration tests. Train IT staff to track, verify, and patch vulnerabilities within set timelines.
- **Digital Forensics (FOR) / Digital Forensics Analyst:** Outsource forensic services for incident investigation and evidence handling. Train the IT manager on preserving logs and maintaining chain-of-custody procedures.

Part C- Security Risk Management Recommendations (based on recommendations from Class Assignments 1-11) – this is the focus of the executive Class Presentation

C1. Security Risk Management Recommendations: Provide the list of recommended Prevention and Response controls, methods and policies and their implementation costs and benefits based on your risk management analysis in Part A for HGA and Part B for your company

Proposed Controls for HGA:

- **New CISO**
- **Missing MOT Controls**
- **2-Factor Authentication**
- **VPN**
- **DMZ**

Risk Prevention Budget: $520000

VPN (Link):

- NordVPN's business option, NordLayer, starts at $10 per month (and $8 per month when paid annually)
- https://www.forbes.com/advisor/business/software/vpn-cost/

- A VPN encrypts remote connections, preventing attackers from intercepting sensitive data transmitted over public or unsecured networks. It also restricts remote access to authorized users only, lowering the risk of network compromise.

2FA(Link):

- $6 per user per month
- https://duo.com/editions-and-pricing (DUO)
- Two-Factor Authentication adds a second verification step, making stolen or guessed passwords useless to attackers. This significantly reduces unauthorized access to sensitive systems and administrative accounts.

NEW CISO:

- A new CISO provides centralized leadership for all cybersecurity strategy, policies, and compliance efforts. This ensures clear accountability and strengthens HGA's ability to detect, respond to, and manage cyber risks.

Missing MOT Controls (Management, Operational, Technical):

- Implementing the missing MOT controls fills critical gaps in policies, processes, and technical safeguards. Together, these controls create a balanced security posture that reduces vulnerabilities caused by weak oversight and inconsistent security practices.

DMZ (Demilitarized Zone):

- A DMZ separates public-facing services from the internal network, limiting attacker movement if a public server is compromised. This containment reduces the likelihood of internal data breaches and protects critical internal systems.

Proposed Controls for HGA:

- **New CISO**
- **Missing MOT Controls**
- **Redundant Server**
- **Mirror Site**

Risk Prevention Budget: $750,000

Redundant Server (Link):

- $5000 ++
- https://www.itsasap.com/blog/server-cost
- A redundant server provides immediate failover capability if the primary server fails, preventing downtime and preserving system availability. This reduces the risk of operational disruption, data loss, or service interruption caused by hardware failure or technical outages.

Mirror Site (Link):

- $300,000 Annually (Hot site)
- https://1111systems.com/blog/are-you-prepared-when-a-disaster-happens/#:~:text=Cold%20site%20%E2%80%93%20Would%20cost%20$50%2C000,systems%20in%20approximately%20an%20hour.
- A mirror site maintains real-time copies of critical systems and data, allowing HGA to restore full operations almost instantly during a disaster. This ensures business continuity and minimizes financial loss by keeping systems accessible even during catastrophic events.

NEW CISO:

- A new CISO provides executive-level leadership and establishes a unified cybersecurity strategy for HGA. This role ensures proper oversight, risk management, and compliance, significantly strengthening the organization's overall security posture.

Missing MOT Controls (Management, Operational, Technical):

- Implementing the missing MOT controls closes critical gaps in policy enforcement, daily security operations, and technical safeguards across the enterprise. These controls collectively reduce vulnerabilities caused by inconsistent procedures, weak configurations, and limited oversight.

Total Budget Estimate for both Proposed Controls for HGA = $520000 + $750,000 =$1270,000

Security Risk Management Recommendations for BrightSmile Dental Group (Fictional)

Proposed Prevention Controls for BrightSmile Dental Group (Fictional):

- Deploy Endpoint Protection and Full-Disk Encryption on All Devices
- Enforce Network Segmentation Between Clinical, Administrative, and Guest Wi-Fi Networks
- Deploy Next-Generation Firewall (NGFW) With IDS/IPS
- Conduct Regular Vulnerability Scans and Patch Updates
- Maintain Redundant Encrypted Backups (On-Site and Cloud-Based)

Risk Prevention Budget: $50000 / Yrs

Deploy Endpoint Protection and Full-Disk Encryption on All Devices:

- Endpoint protection tools monitor for malware and suspicious activity in real time, stopping attacks before they spread. Full-disk encryption prevents unauthorized data access if a laptop or workstation is stolen, lost, or improperly accessed.
- https://solutions.trustradius.com/buyer-blog/endpoint-security-pricing/
- **Budget: $ 2000 /Yrs**

Enforce Network Segmentation Between Clinical, Administrative, and Guest Wi-Fi Networks:

- Separating internal networks into VLANs prevents attackers or malware from moving laterally between systems if one device becomes compromised. This segmentation ensures that clinical systems and PHI remain isolated from guest devices and less secure administrative workstations.
- https://www.akamai.com/glossary/what-is-network-segmentation

- **Budget: $5000 – $10000 /Yrs**

Deploy Next-Generation Firewall (NGFW) With IDS/IPS:

- A Next-Generation Firewall with intrusion detection and prevention blocks malicious traffic, detects suspicious behavior, and stops attacks before they reach internal systems. This prevents external intrusions, ransomware delivery attempts, and unauthorized access to PHI.
- **https://www.esecurityplanet.com/products/top-ngfw/**
- **Budget: $ 10000 - $30000 /Yrs**

Conduct Regular Vulnerability Scans and Patch Updates:

- Routine scanning identifies outdated software, missing patches, and exploitable vulnerabilities before cybercriminals can take advantage of them. A structured patch management program ensures all systems, including the EHR and imaging devices, are kept secure and up to date.
- **https://www.vikingcloud.com/blog/vulnerability-assessment-cost**
- **Budget: $1000 - $5000 / Yrs**

Maintain Redundant Encrypted Backups (On-Site and Cloud-Based):

- Redundant encrypted backups ensure that all patient data, imaging files, and billing information can be restored in the event of a ransomware attack or system failure. This reduces downtime and prevents permanent data loss that could interrupt patient care.
- **https://aws.amazon.com/backup/pricing/**
- **Budget: $500 - $1000 / Yrs**

Proposed Response Controls for BrightSmile Dental Group (Fictional):

- Provide Recurring Security Awareness and HIPAA Training to All Employees
- Automated Containment Tools (EDR Isolation, Firewall Blocking Rules)
- Centralized Log Collection and Real-Time Security Monitoring
- Appoint an Incident Response Lead or Contract an MSSP
- Formal Incident Response Plan (IRP)

Risk Response Budget: $40000 / Yrs

Provide Recurring Security Awareness and HIPAA Training to All Employees:

- Regular training teaches employees how to identify phishing emails, social engineering attempts, and unsafe practices that could expose PHI. Improving staff awareness significantly reduces human error, which is one of the most common causes of healthcare data breaches.
- https://www.jerichosecurity.com/blog/how-much-cyber-security-training-cost#:~:text=Coordinating%20with%20the%20security%20awareness,data%20breach%20is%20$3.86%20million.
- **Budget: $1000 - $3000 / Yrs**

Automated Containment Tools (EDR Isolation, Firewall Blocking Rules):

- Endpoint Detection and Response tools can automatically isolate infected devices from the network to prevent malware from spreading. Dynamic firewall rules allow the clinic to block malicious IPs or traffic patterns immediately once an attack is identified.
- https://qualysec.com/endpoint-protection-cost/
- **Budget: $3000- $5000 / Yrs**

Centralized Log Collection and Real-Time Security Monitoring:

- Centralized logging combined with 24/7 monitoring allows rapid detection of unauthorized access, unusual network traffic, or attempted compromise of EHR and billing systems. Early detection enables quicker containment and reduces the impact of cyberattacks.
- https://www.buchanan.com/managed-siem-pricing/
- **Budget $10000 - $30000 / Yrs**

Appoint an Incident Response Lead or Contract an MSSP:

- Designating an IR Lead or outsourcing to a Managed Security Service Provider ensures that trained professionals handle active threats quickly and effectively. This reduces the likelihood of the attack spreading and minimizes damage to patient data and clinical systems.
- **https://blog.rsisecurity.com/how-much-does-managed-security-services-cost/#:~:text=According%20to%20one%20study%2C%20the,that's%20potentially%20a%20huge%20spread.**
- **Budget: $5000 - $10000 / Yrs**

Formal Incident Response Plan (IRP):

- **A formal Incident Response Plan ensures the clinic has clear, step-by-step procedures for identifying, containing, and recovering from security incidents such as ransomware or PHI breaches. This structured approach reduces confusion during emergencies and shortens the time needed to restore safe operations.**
- **https://complianceforge.com/product/integrated-incident-response-program/**
- **Budget: $10000 - $40000 / Yrs**

Total Budget Estimate (Annually) = $50000 + $40000 =$90000

C2. Provide the total cost and total risk reduction benefit in $ due to the recommended controls, methods and policies based on your security risk management analysis in Parts A and B.

HGA: Total Cost of Recommended Control Implementation = Prevention Control + Response Control

- $520000 + $750000 =$1270000

Reduction = Initial Risk Impact – Risk After Implementing Strategy

Risk Reduction Benefit From Prevention Controls = $798765

Risk Reduction Benefit from Response Controls = $ 567899

The cybersecurity assessment conducted for HGA identified significant weaknesses in governance, access control, network security, and disaster recovery capabilities, all of which posed considerable risks to the organization' s operational stability and data integrity. To address these vulnerabilities, a comprehensive set of prevention and response controls was recommended to improve HGA' s overall security posture. The prevention controls, such as hiring a new CISO, implementing missing Management, Operational, and Technical (MOT) controls, enforcing 2- Factor Authentication, deploying a secure VPN, and establishing a DMZ greatly enhance the organization' s ability to deter, detect, and mitigate cyber threats before they escalate. These measures offer a risk- reduction benefit of $798,765, demonstrating the effectiveness of proactive governance, improved authentication practices, and stronger perimeter defenses.

The response controls further boost HGA' s resilience by introducing redundant server capabilities and a fully operational mirror site, ensuring that critical systems can be restored quickly in the event of a disaster or major failure. This significantly improves business continuity and lowers costly downtime, resulting in an additional risk- reduction benefit of $ 567,899. Together, the prevention and response controls provide a total risk- reduction benefit of $1,366,664, directly supporting HGA' s strategic goal of minimizing cybersecurity risk and maintaining continuous operations.

When compared to the total implementation cost of $1,270,000 with $520,000 allocated to prevention controls and $ 750, 000 to response controls the recommended security strategy offers a positive Return on Investment (ROI) of approximately 7. 61%. This ROI reflects the financial gains from reduced exposure, improved resilience, and enhanced operational continuity. Beyond the direct monetary benefits, the implemented controls deliver long- term advantages by reducing regulatory exposure, safeguarding sensitive systems, and establishing a more mature cybersecurity posture across the organization.

In conclusion, the recommended controls for HGA represent a cost- effective and strategic investment that not only addresses current vulnerabilities but also prepares the organization to defend against future threats. The clear alignment between costs, risk- reduction benefits, and enhanced resilience confirms that adopting these controls will significantly improve HGA' s security posture and ensure more reliable, secure, and compliant operations moving forward.

BrightSmile Dental Group (Fictional): Total Cost of Recommended Control Implementation = Prevention Control + Response Control

- $50000 + $40000 =$90000

Total Risk Reduction Benefit (Estimated) = $350000 - $750000

The security assessment for BrightSmile Dental Group (Fictional) identified significant gaps across endpoint security, network segmentation, firewall protection, vulnerability management, data backup resilience, and incident response readiness. To address these vulnerabilities, a targeted set of prevention and response controls was recommended, each chosen for its effectiveness and affordability within the practice' s annual security budget. The prevention controls including endpoint protection with full- disk encryption, segmentation of clinical and guest networks, deployment of a Next- Generation Firewall with IDS/IPS, routine vulnerability scanning and patching, and maintaining redundant encrypted backups collectively strengthen the confidentiality, integrity, and availability of Protected Health Information (PHI). These controls greatly reduce the risk of ransomware incidents, unauthorized access, wireless intrusions, and data loss events in a cost- effective way.

The response controls further enhance the organization' s ability to react quickly and effectively during security incidents. Recurring security awareness and HIPAA training help reduce breaches caused by human error, while automated containment tools enable rapid device isolation to prevent threats from spreading. Centralized log collection with real- time monitoring improves early detection of suspicious activity, and establishing an Incident Response Lead or contracting a Managed Security Service Provider ensures expert support when threats occur. A formal Incident Response Plan offers clear procedures for identifying, containing, and recovering from incidents, supporting consistent action under pressure. Together, these response controls strengthen operational resilience and maintain patient trust during adverse events.

From a financial point of view, the recommended controls fit within the annual budget, totaling $90,000, with $50,000 allocated to prevention measures and $ 40, 000 for response capabilities. The estimated risk-reduction value of $350,000 to $750,000 shows that these security improvements provide significant savings by reducing potential losses from data breaches, operational downtime, regulatory penalties, and system recovery costs. Based on these figures, the Return on Investment (ROI) ranges from 288% to 733%, confirming that the security upgrades are both operationally essential and financially beneficial. Overall, the combined prevention and response measures give BrightSmile Dental Group (Fictional) a strong, sustainable cybersecurity posture that protects patient data, maintains operational continuity, and ensures compliance with HIPAA and industry best practices.

C3. Compare your proposed security controls, methods and policies budget for HGA (which is based on security risk assessment in Part A) with the proposed security controls, methods and policies budget for your company (which is based on security risk implementation plan in Part B), comparing the two companies at a high level on the following security risk management areas:

	HGA	BrightSmile Dental Group (Fictional)
Industry	Government Finance and Accounting	Sole Proprietorship, Small Private Dental Practice
Mission	Securely transfer government funds and protect sensitive financial and personnel data	The mission of BrightSmile Dental Group (Fictional) is to provide compassionate, high-quality dental care that promotes long-term oral health and patient well-being.
Geographic Presence	Nationwide	Single location in San Diego, CA
Number of employees	1000	50+
Network Topology	Provided in Appendix	Provided in Appendix
Critical Assets in $	$3,045,000 or $3.04M	$1.5 Million - $5 Million+
Threat Agents	Cybercriminal Organizations Nation-State Actors Hacktivists Malicious Insider Threats Third-Party Vendors and Business Associates	Cybercriminals targeting healthcare practices Insider threats (malicious or negligent employees) Phishing and social engineering actors Malware authors exploiting unpatched systems Rogue insiders from cleaning crews or after-hours staff
Attack Tree Scenarios	Provided Below	Provided Below

Top 3 Vulnerabilities and Exploitation Probabilities	Lack of Strong Access Controls and MFA (75%) Inadequate Disaster Recovery and Failover Capabilities (60%) Missing Management, Operational, and Technical (MOT) Controls (55%)	Weak or Unsecured Wireless Networks (80%) Lack of Endpoint Protection and Full-Disk Encryption (70%) Limited Logging, Monitoring, and Incident Response (50%)

Assets Vulnerabilities and consequential Asset Risks	**Electronic Health Records (EHR) System:** The EHR system at HGA is vulnerable because of weak access controls and the absence of mandatory multi-factor authentication for users accessing sensitive health data. This exposes the organization to the risk of unauthorized access, insider misuse, credential theft, and potential HIPAA violations. **Core Network Infrastructure and Servers:** HGA's core network infrastructure and servers are at risk due to missing Management, Operational, and Technical (MOT) controls, outdated device configurations, and insufficient continuous monitoring. These weaknesses heighten the likelihood of malware infiltration, unauthorized system compromise, and lateral movement across internal networks. **Business Continuity & Disaster Recovery Systems:**	**Patient Dental Records & Imaging Systems:** The patient dental records and imaging systems are vulnerable due to the lack of endpoint protection and the absence of full-disk encryption on the devices that store or access PHI. As a result, these weaknesses create a significant risk of PHI exposure in the event of device theft, ransomware infection, or unauthorized access by internal or external threat actors. **Wi-Fi and Network Infrastructure:** The Wi-Fi and overall network infrastructure are at risk because of weak wireless security practices, including shared passwords, outdated WPA2 encryption, and insecure configuration settings. These vulnerabilities increase the likelihood of unauthorized access, eavesdropping on network traffic, and potential entry points into the clinical network where sensitive systems reside. **Workstations & Clinical Applications:** The workstations and clinical applications face vulnerabilities due to inconsistent

	The business continuity and disaster recovery systems are vulnerable because the organization lacks redundant server capacity and does not maintain a mirror site for rapid failover. This deficiency exposes HGA to the risk of prolonged downtime, disrupted clinical operations, and financial loss during outages or ransomware events.	patching, limited security monitoring, and the lack of centralized log analysis. These deficiencies raise the risk of malware infections, delay the detection of intrusions, and contribute to overall system instability that can disrupt clinical operations.

Recommended Prevention Controls	**Multi-Factor Authentication (MFA):** Protects EHR and administrative systems by preventing unauthorized access even if credentials are stolen. **VPN for Remote Access** : Ensures encrypted remote connectivity, blocking unauthorized or insecure external access. **Next-Generation Firewall (NGFW) with IDS/IPS:** Detects and blocks malicious traffic, preventing network compromise. **Network Segmentation**: Separates clinical, administrative, and public-facing systems to prevent lateral movement. **Endpoint Security and Full-Disk Encryption:** Protects servers and administrative endpoints from malware and data theft.	**Regular Vulnerability Scanning & Patch Updates**: Ensures dental records and imaging data can be restored after ransomware or system failure. **Encrypted Redundant Backups:** Ensures dental records and imaging data can be restored after ransomware or system failure. **Security Awareness & HIPAA Training:** Reduces human error by teaching staff to recognize phishing and follow safe data-handling practices. **Network Segmentation (Clinical, Admin, Guest Wi-Fi):** Prevents attackers from moving from guest or administrative networks into PHI systems. **Endpoint Protection and Full-Disk Encryption :** Protects patient data on devices and prevents unauthorized access from theft or compromise.

Top 3 Risk Impacts	**Loss of access to critical medical systems**, resulting in delayed or disrupted patient care. **Exposure or theft of PHI**, leading to regulatory fines, legal liability, and reputational harm. **Extended operational downtime**, causing productivity loss, financial damage, and instability of clinical workflows.	**Compromise of patient dental records**, resulting in HIPAA violations and loss of patient trust. **Ransomware infection**, causing loss of access to imaging systems and operational disruption. **Unauthorized access through weak W**i-Fi or unpatched systems, leading to data exposure and system instability.

Assets Risk Impacts and consequential Asset Risks	**Electronic Health Records (EHR) System:** A breach or outage of the EHR system would directly compromise patient care by preventing clinicians from accessing essential medical records, orders, and documentation. This risk could lead to patient safety issues, regulatory penalties, and a long-term loss of trust from patients and partners. **Core Network Infrastructure and Servers:** If the network infrastructure were compromised, attackers could gain persistent access, disrupt services, or deploy ransomware across connected systems. This would result in widespread operational outages, compromised communication channels, and significant financial losses. **Business Continuity & Disaster Recovery Systems:** Failure in business continuity or lack of failover capability would leave HGA vulnerable to prolonged outages during cyberattacks or system failures. This leads to major clinical disruptions, inability to resume services quickly, and escalating financial and operational damage.	**Patient Dental Records & Imaging Systems:** A compromise of dental records or imaging systems would expose PHI and disrupt clinical procedures, causing regulatory penalties and reputational damage. The inability to access patient history or imaging could delay care and affect treatment accuracy. **Wi-Fi and Network Infrastructure:** Weak wireless configurations could allow unauthorized users to infiltrate the network, intercept traffic, or pivot into clinical systems. This risk directly threatens PHI confidentiality and can lead to ransomware delivery or network-wide compromise. **Workstations & Clinical Applications:** Unpatched workstations and insufficient monitoring increase the likelihood of malware infections and undetected intrusions. These risks can destabilize clinical operations, cause system outages, and lead to corrupted or inaccessible patient data.

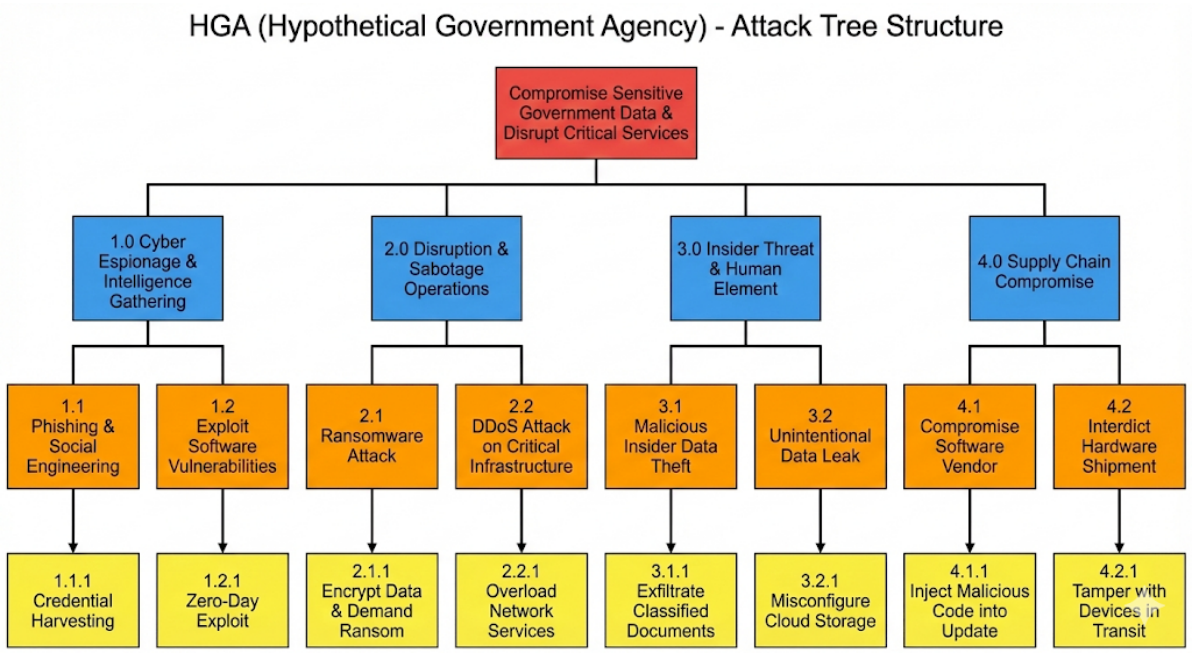
Recommended Response Controls	**Establish a Formal Incident Response Plan (IRP):** An IRP ensures staff follow a structured, step-by-step process for identifying, containing, and recovering from cyber incidents. **Implement Centralized Log Collection and Real-Time Monitoring:** Centralized monitoring enables early detection of suspicious activity and rapid escalation of security events. **Automate Containment with EDR Isolation and Firewall Blocking Rules:** These tools isolate infected devices immediately and block malicious traffic, preventing widespread compromise. **Deploy Redundant Servers and a Real-Time Mirror Site:** Redundancy ensures critical systems remain accessible during failures or attacks, reducing downtime. **Designate an Incident Response Lead or Contract an MSSP:** Trained professionals provide rapid threat handling and limit the scope and severity of incidents.	**Provide Regular Security Awareness and HIPAA Training:** Training helps staff recognize phishing attempts, improper PHI handling, and early signs of compromise. **Implement Automated Containment Tools (EDR and Firewall Blocking):** EDR isolation removes infected devices from the network instantly, reducing malware spread. **Enable Centralized Logging and 24/7 Monitoring:** This improves visibility, allowing early detection of suspicious activity and rapid response. **Appoint an Incident Response Lead or Contract an MSSP:** An IR Lead or MSSP ensures expert handling of incidents and reduces response time. **Create a Formal Incident Response Plan (IRP):** A structured IRP guides the organization's response to ransomware, data breaches, and system failures, reducing confusion and downtime.
Residual Asset Risks (Post Controls) in $	$980,000	$300,000
Risk Prevention Budget	$520,000	$50,000
Risk Response Budget	$750,000	$40,000

Total Security Budget	$1270,000	$90,000
ROI (Total Security Risk Improvement)	$980,000 ROI: 77.2%	$300,000 ROI: 3.33%
ROA ($Budget/$Critical Assets)	$1270,000/ $3045,000 =0.42(42%)	$90,000/$1500,000 =0.06(6%)
ROHC($Budget/Employee)	$1270,000/1000 = $1270 per employee	$90,000/50 (min) =$18,000 per employee

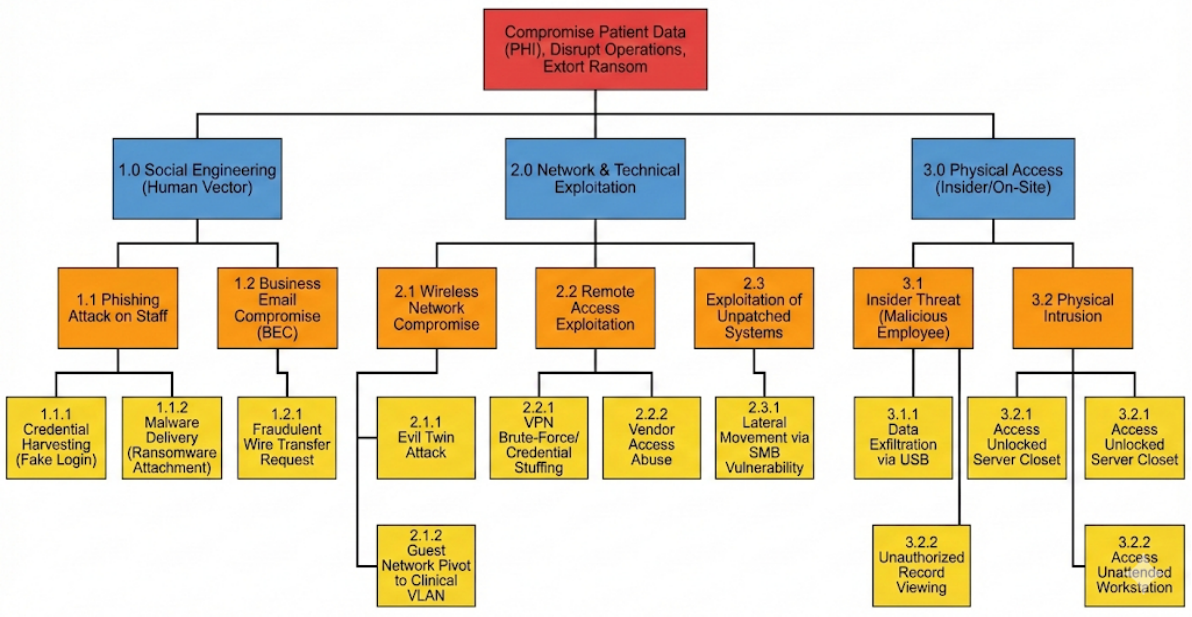
Cybersecurity Workforce Recommendations	**Cyber Defense Analyst (CDA):** HGA requires full-time analysts to monitor security events, investigate alerts, and respond to internal and external threats in real time. **Systems Administrator (ADM):** HGA needs skilled administrators to manage servers, patching schedules, access provisioning, backups, and secure configuration baselines. **Network Operations Specialist (NET):** This role ensures secure operation of the network infrastructure, including firewalls, segmentation, VPN, IDS/IPS, and bandwidth management. **Security Control Assessor (SCA):** An SCA is essential to validate security controls, conduct risk assessments, and ensure continuous compliance with healthcare and federal security frameworks. **Incident Response Specialist (CIR):** A dedicated specialist is needed to conduct forensic analysis, containment, eradication, and recovery during cyber incidents especially ransomware outbreaks.	**Part-Time or Contract IT Security Manager:** A contract-based security manager can oversee compliance, manage risk assessments, and ensure HIPAA security standards are consistently met. **Managed Security Service Provider (MSSP):** Outsourcing monitoring, logging, and incident response to an MSSP provides 24/7 protection without requiring full-time internal staff. **Technical Support Specialist (STS):** A support technician is needed to handle workstation setup, patching, troubleshooting, and secure configuration of clinical devices. **Network Operations Support (External Vendor):** A contracted network specialist can maintain firewalls, secure Wi-Fi, manage segmentation, and ensure proper configuration of network controls. **Security Awareness and HIPAA Training Coordinator (Internal or Vendor):** This role ensures employees receive consistent training on phishing, safe data handling, and regulatory compliance critical for preventing human-error breaches.

Attack Tree

HGA Attack Tree:



BrightSmile Dental Group (Fictional) Attack Tree:



Budget Calculations for HGA:

Initial Risk (Before Controls): $3,045,000

Risk Reduction (Post Controls): $980,000 (From prevention + Response Measures)

Residual Asset Risk= Initial Risk – Risk Reduction

- **Residual Risk** = $3,045,000 - $980,000 =$2947000

Risk Prevention Budget : $520,000

Risk Response Budget : $750,000

Total Security Budget = Prevention Budget + Response Budget

- $520,000 + $750,000 = $1270,000

Return on Investment(ROI) = Risk Reduction /Total Security Budget

- $980,000/$1270,000 = 77.2%

Return on Assets (ROA) = Total Security Budget / Total Critical Assets

- $1270,000/ $3,045,000 = 42%

Return on Human Capital (ROHC) = Total Security Budget / Number of Employees

- $1270,000/1000 = $1270 per employee

Budget Calculations for BrightSmile Dental Group (Fictional):

Initial Risk (Before Controls): $1500,000

Risk Reduction (Post Controls): $300,000 (From prevention + Response Measures)

Residual Asset Risk= Initial Risk – Risk Reduction

- **Residual Risk** = $1500,000 - $300,000 =$1200,000

Risk Prevention Budget : $50,000

Risk Response Budget : $40,000

Total Security Budget = Prevention Budget + Response Budget

- $50,000 + $40,000 = $90,000

Return on Investment(ROI) = Risk Reduction /Total Security Budget

- $300,000/$90,000 = 3.33%

Return on Assets (ROA) = Total Security Budget / Total Critical Assets

- $90,000/ $1500,000 = 6%

Return on Human Capital (ROHC) = Total Security Budget / Number of Employees

- $90,000/50 (min) =$18,000 per employee

	HGA	BrightSmile Dental Group (Fictional)
Residual Asset Risk	$2947000	$1200,000
Risk Prevention Budget	$520,000	$50,000
Risk Response Budget	$750,000	$40,000
Total Security Budget	$1270,000	$90,000
Return on Investment(ROI)	77.2%	3.33%
Return on Assets (ROA)	42%	6%
Return on Human Capital (ROHC)	$1270 per employee	$18,000 per employee

Conclusion and Recommendation for BrightSmile Dental Group (Fictional):

After completing this security risk assessment for BrightSmile Dental Group (Fictional), I found that although the organization has taken meaningful steps to strengthen its cybersecurity posture, it still faces a significant level of exposure due to the sensitive nature of patient data and the increasing targeting of small healthcare providers. My analysis shows that the initial estimated risk for the practice was $1,500,000, and through the implementation of both prevention and response controls, the organization was able to reduce this exposure by $300,000. Even with this reduction, a residual risk of $1,200,000 remains, which emphasizes the need for continued investment and further enhancement of security measures.

With a total security budget of $90,000 split between $50,000 for preventive controls and $40,000 for response measures the practice demonstrates a thoughtful and cost-effective approach to managing risk. This investment yields a 3.33% ROI, indicating that the security controls are generating real value by lowering financial exposure. The 6% Return on Assets (ROA) and $18,000 Return on Human Capital (ROHC) highlight that this spending aligns with the size of the practice and its workforce. However, the remaining risk level highlights the need for ongoing development of its security framework.

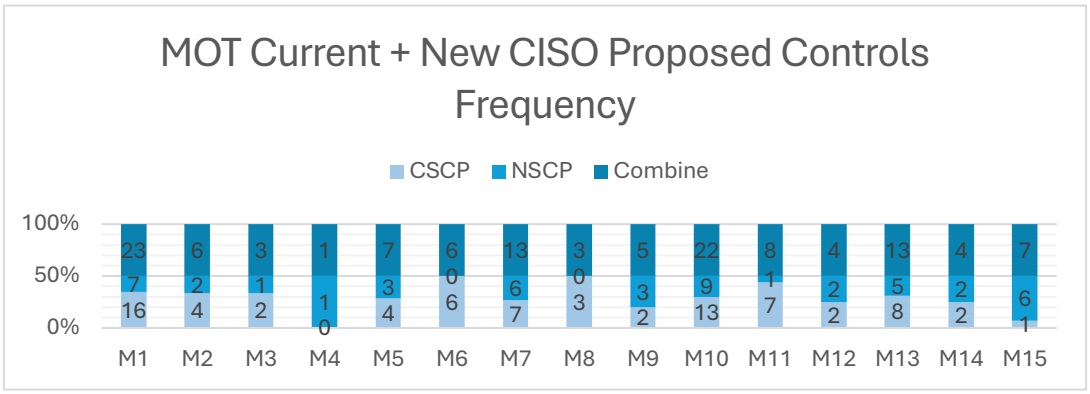
Moving forward, the best steps for BrightSmile Dental Group (Fictional) involve focusing on security areas that offer the highest impact and return. First, I recommend strengthening the practice's incident response and detection capabilities, since response-based controls tend to provide higher ROI and are crucial in limiting damage during an attack. Implementing centralized logging, 24/7 monitoring, and automated containment tools like EDR isolation will significantly reduce the chances of prolonged compromise. Second, it is vital to improve endpoint security and ensure that all clinical devices including laptops, imaging systems, and front-desk workstations use full-disk encryption and modern protection solutions. Third, enhancing network defenses by upgrading Wi-Fi security to WPA3, enforcing strong segmentation between clinical and guest networks, and maintaining updated firewall rules will greatly lower the practice's attack surface. Finally, continuous employee training should be regarded as a core requirement, as human error remains one of the leading causes of healthcare data breaches.

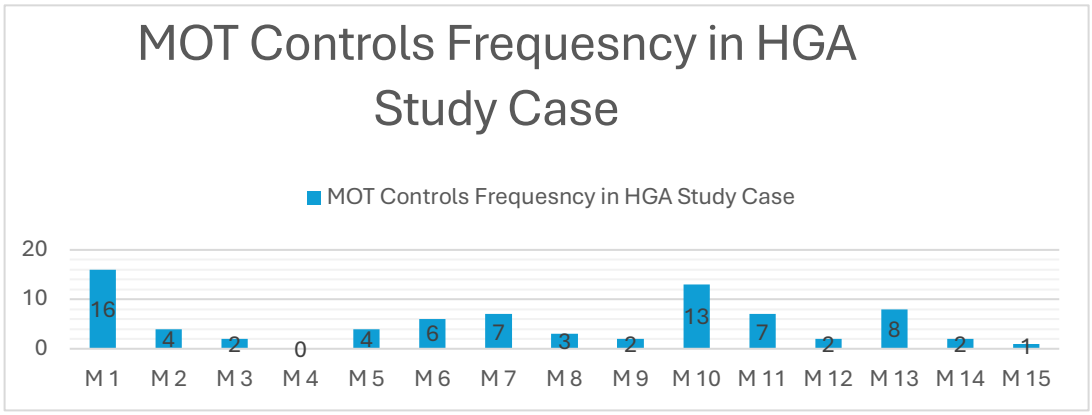
In conclusion, this assessment shows that BrightSmile Dental Group (Fictional) is making progress, yet ongoing commitment is essential to manage residual risks and safeguard patient data. By continually investing in high-impact response capabilities, modernizing device and network security, and emphasizing

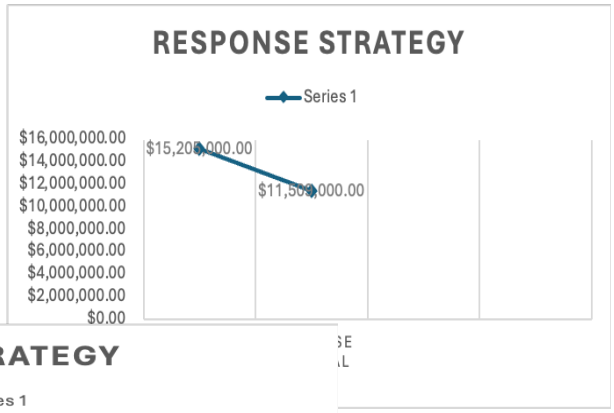
cybersecurity awareness among staff, the practice will be better equipped to reduce future threats, ensure regulatory compliance, and maintain patient trust.

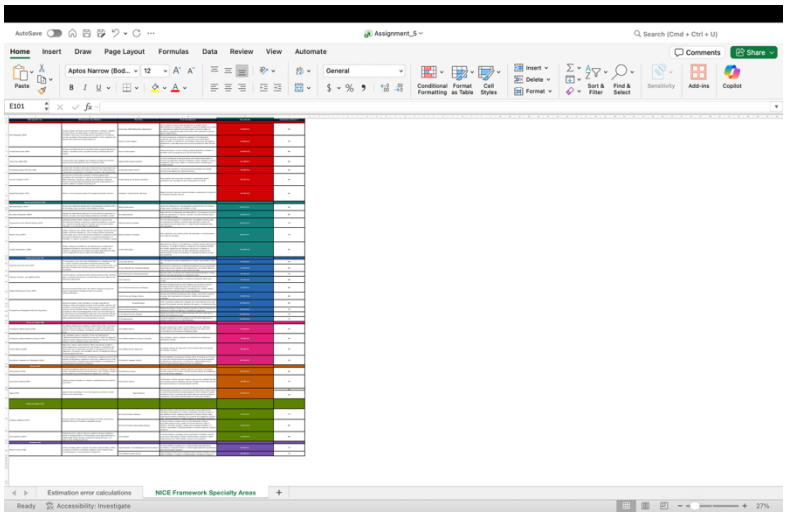
Part D

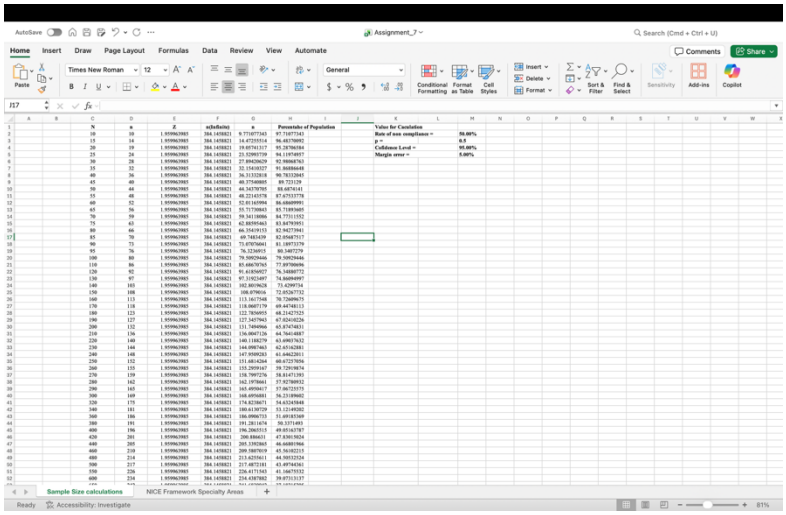
Appendix 1: All MS-Excel spreadsheet models

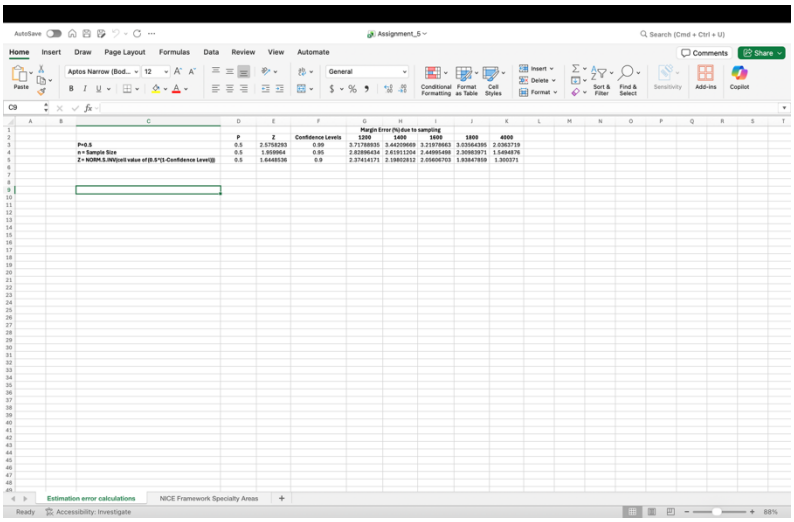












Appendix 2: Any data, analysis, controls or policies not included above

- **HGA Assets List**

Asset Number	Asset Name	Description	Asset Value
A1	Payroll System & Financial Resources	Critical system managing US Government fund transfers including paychecks, direct deposits, and tax withholdings. Financial integrity essential to agency mission and employee welfare.	**95**
A2	Employee Master Database	Comprehensive personnel database stored on mainframe containing service dates, leave balances, salary information, W-2 data, and other Privacy Act protected information.	**90**
A3	Time and Attendance Application	Weekly timesheet processing system including data entry, validation, supervisor approval, and mainframe submission. Core component of payroll fraud prevention.	**85**
A4	Personnel Information & Records	Employment records, background investigations, performance evaluations, correspondence, and other human resources data requiring confidentiality protection.	**80**
A5	Draft Regulations & Policy Documents	Pre-publication regulatory documents and internal policy drafts with potential competitive and policy implications if prematurely disclosed.	**75**
A6	LAN Server Infrastructure	Central processing platform providing shared storage, application execution, email services, and network connectivity for distributed operations.	**70**
A7	Contracting & Procurement Documents	Vendor agreements, pricing information, procurement strategies, and competitive bidding documents with financial sensitivity.	**65**
A8	Network Infrastructure (Router/WAN)	Communication equipment including Internet router, WAN connection, and packet filtering systems enabling external connectivity.	**60**
A9	Personal Computer Workstations	Individual desktop systems with local storage, processing capability, and network connectivity distributed throughout agency facilities.	**55**
A10	Internal Business Communications	Inter-departmental correspondence, meeting records, administrative memos, and routine business documentation.	**50**
A11	HGA Reputation & Public Trust	Agency credibility with Congress, citizens, and other federal agencies. Intangible but mission-critical asset affecting operational effectiveness.	**85**

- **List of threats**

Threat ID	Threat Name	Description
T1	Payroll Fraud	Fraudulent timesheet submission for unworked hours, falsifying service dates for retirement benefits, creating

		fictitious employee records. Historical attempts primarily from within HGA.
T2	Payroll Errors	Data entry mistakes, failure to process personnel changes timely, accidental corruption of time and attendance data, inter-agency coordination failures.
T3	In Interruption of Operations	Unauthorized access to employee databases for Power outages from aging infrastructure, equipment malfunctions, natural disasters, malicious disruption targeting time-critical payroll processing.
T4	Information Disclosure/Brokerage	Legitimate users accessing employee database to sell information to private investigators, employment recruiters, press for commercial gain.
T5	Network-Related Threats	External penetration via Internet, password guessing, unauthorized dial-up access, exploitation of email utility bugs for administrator privileges.
T6	Accidental Loss/Release of Information	Unintentional exposure of disclosure-sensitive personnel data through poor handling, unsecured storage, inadvertent transmission.
T7	Theft	Physical theft of computer equipment, storage media, documents containing sensitive information from agency facilities.
T8	Virus Contamination	Malware infections causing data corruption, system disruption, unauthorized access through infected software or removable media.
T9	Natural Disaster	Fires, floods, storms causing extended outages and data loss affecting critical business operations.
T10	Unauthorized Telecommunications Access	Eavesdropping on dial-up connections, WAN communications, modem pool exploitation for unauthorized system access.

- **List of Security Vulnerabilities**

Vulnerability ID	Vulnerability Name	Description
V1	Clear-text Password Transmission	User passwords broadcast unencrypted over LAN during authentication, easily captured by network sniffing tools or malicious software.
V2	Immature Server Operating System	LAN server uses recently deployed OS with known security vulnerabilities and insufficient hardening against privilege escalation attacks.
V3	Inadequate Physical Security Compliance	Widespread non-compliance with document storage policies, unlocked computers containing sensitive data, and poor after-hours security practices.
V4	Email System File Access Vulnerability	Email utility allows users to attach any accessible file to outgoing messages, enabling data exfiltration via Internet or dial-up connections.

V5	Weak Administrative Controls	Delayed security patch installation, insufficient compliance monitoring, and lack of regular security awareness training updates.
V6	Mainframe Authentication Weaknesses	Shared mainframe system relies on password-only authentication serving multiple agencies with varying security standards, creating attack vectors.
V7	WAN Data Interception	Time and attendance data transmitted over WAN vulnerable to tampering at relay switches, potential HGA-WAN provider collusion.
V8	Unencrypted LAN Communications	Information broadcast to all LAN connection points without encryption, trivial eavesdropping with widely available sniffer programs.
V9	Inadequate PC Backup Procedures	Many users store significant data locally without backing up, leading to frequent data loss incidents.
V10	Virus Prevention Non-compliance	COG personnel not routinely running virus scanners despite monthly requirements, only during publicized scares.
V11	Untested Contingency Plans	Alternative site processing capabilities never verified despite annual testing requirements, may prove illusory during emergencies.
V12	Insufficient Audit Logging	Systems lack capabilities to track attacker activities, cannot accurately gauge extent of network penetrations when they occur.

- **Current Security Controls and Policies**

CSCP Number	Category	Description
CSCP1	General Purpose	Computer Security Manual implementing OMB A-130, Computer Security Act of 1987, Privacy Act, OMB A-123/A-127, Federal Managers' Financial Integrity Act
CSCP2	General Purpose	Need-to-know access policy limiting information access to job requirements only
CSCP3	General Purpose	Written authorization required from department supervisors before system access
CSCP4	General Purpose	Mandatory security awareness training before account activation
CSCP5	General Purpose	Acknowledgment forms requiring users to understand security responsibilities

CSCP6	General Purpose	Background investigations and personnel screening procedures
CSCP7	General Purpose	Only System Administrators authorized to establish login IDs and passwords
CSCP8	General Purpose	Password selection and periodic change requirements with penalties for non-compliance
CSCP9	Protection Against Unauthorized Execution	Separation of duties requiring two-person approval for payroll transactions
CSCP10	Protection Against Unauthorized Execution	LAN server elementary access control lists limiting file and program access
CSCP11	Protection Against Unauthorized Execution	Group-oriented controls allowing team-based access to sensitive files
CSCP12	Protection Against Unauthorized Execution	Password-based identification and authentication for server access
CSCP13	Protection Against Unauthorized Execution	Special access control privileges required for WAN interface access
CSCP14	Protection Against Unauthorized Execution	Time and attendance application restricted to specific PCs and business hours
CSCP15	Protection Against Payroll Errors	Automated data validation checking for invalid employee IDs and implausible hours
CSCP16	Protection Against Payroll Errors	Dual data entry system for time sheets with discrepancy detection
CSCP17	Protection Against Payroll Errors	Weekly paper timesheet submission with supervisor approval
CSCP18	Protection Against Payroll Errors	Exception reporting for negative leave balances and out-of-range values
CSCP19	Protection Against Payroll Errors	Personnel action forms required one week before payroll processing
CSCP20	Protection Against Accidental	Nightly server disk backups to magnetic tape with weekly offsite storage

	Corruption or Loss of Payroll Data	
CSCP21	Protection Against Accidental Corruption or Loss of Payroll Data	One-year online retention with three-year archive for time and attendance data
CSCP22	Protection Against Accidental Corruption or Loss of Payroll Data	Read-only access automatically set for submitted payroll files
CSCP23	Protection Against Accidental Corruption or Loss of Payroll Data	WAN communications protocols with error checking for data transmission
CSCP24	Protection Against Accidental Corruption or Loss of Payroll Data	Pre-payroll validation reports identifying missing agency data
CSCP25	Protection Against Interruption of Operations	Computer Operations Group (COG) responsible for system management
CSCP26	Protection Against Interruption of Operations	Spare equipment inventory (10 PCs, spare server, disk drives, LAN cable)
CSCP27	Protection Against Interruption of Operations	Emergency LAN cabling procedures for severed connections
CSCP28	Protection Against Interruption of Operations	Controlled software installation (COG-approved licensed packages only)
CSCP29	Protection Against Interruption of Operations	Monthly virus scanning requirements with incident reporting
CSCP30	Protection Against	Annual contingency plan testing requirements

	Interruption of Operations	
CSCP31	Protection Against Interruption of Operations	Alternative site agreements with nearby agencies for emergency operations
CSCP32	Protection Against Interruption of Operations	Application priority procedures for degraded capacity situations
CSCP33	Protection Against Interruption of Operations	Backup service capacity for 100+ simultaneous users
CSCP34	Protection Against Disclosure or Brokerage of Information	Mandatory locked file cabinet/drawer storage for sensitive papers
CSCP35	Protection Against Disclosure or Brokerage of Information	PC key locks installed on all computers with locking requirements
CSCP36	Protection Against Disclosure or Brokerage of Information	Office locking requirements for overnight protection
CSCP37	Protection Against Disclosure or Brokerage of Information	Approved storage containers with key control limited to document owners
CSCP38	Protection Against Disclosure or Brokerage of	Building security with guard force access controls
CSCP39	Protection Against Disclosure or Brokerage of Information	Server audit log review by COG with security violation reporting
CSCP40	Protection Against Network-Related Threats	Router packet filtering allowing only email traffic between LAN and Internet
CSCP41	Protection Against	Dial-up access restricted to email functions only

	Network-Related Threats	
CSCP42	Protection Against Network-Related Threats	Administrator console exclusive access for server configuration
CSCP43	Protection Against Network-Related Threats	Incident Handling Team for security breach coordination
CSCP44	Protection Against Network-Related Threats	Vendor security patch installation procedures
CSCP45	Protection Against Network-Related Threats	Security configuration validation utilities
CSCP46	Protection Against Risks from Non-HGA Computer Systems	External system authorization required from application owner and COG Manager
CSCP47	Protection Against Risks from Non-HGA Computer Systems	Written safeguarding commitments required from controlling organizations
CSCP48	Protection Against Risks from Non-HGA Computer Systems	Internet usage policy allowing email but prohibiting proprietary data transmission
CSCP49	Protection Against Risks from Non-HGA Computer Systems	Information protection requirements commensurate with HGA-designated value

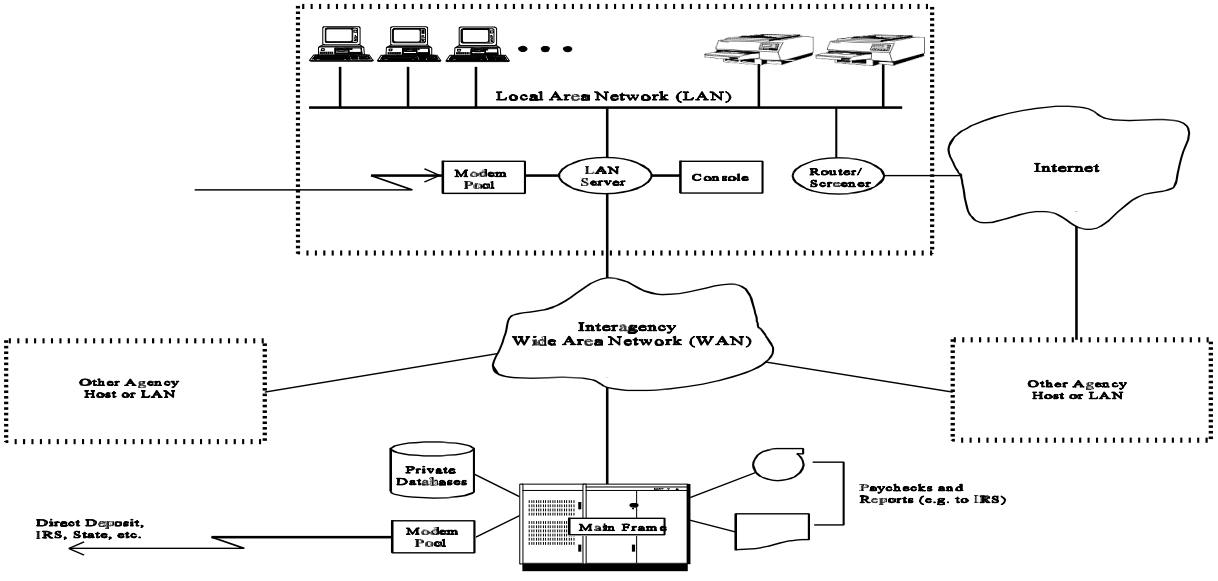
- **List of New Security Controls and Policies (NSCP)**

NSCP Number	Category	Description
NSCP1	Payroll Fraud Mitigation	One-time password system using programmable smart tokens for Time and Attendance Clerks and Supervisors

NSCP2	Payroll Fraud Mitigation	Public key cryptographic signatures for time and attendance data
NSCP3	Payroll Fraud Mitigation	Improved monitoring of LAN server's access control configuration
NSCP4	Payroll Fraud Mitigation	Management decision to maintain current supervisory review procedures
NSCP5	Payroll Error Mitigation	Regular audits of paperwork handling procedures
NSCP6	Payroll Error Mitigation	Enhanced compliance framework with defined consequences
NSCP7	Payroll Error Mitigation	Secondary benefit of digital signature system
NSCP8	Continuity of Operations	Periodic internal training for COG personnel
NSCP9	Continuity of Operations	Mandatory testing of emergency procedures
NSCP10	Continuity of Operations	Alternative processing using magnetic tape
NSCP11	Continuity of Operations	High-level review of mainframe contingency plans
NSCP12	Continuity of Operations	Enhanced compliance with existing virus prevention procedures
NSCP13	Continuity of Operations	Quarterly email reminders for PC users
NSCP14	Continuity of Operations	Regular backup for critical PCs
NSCP15	Information Disclosure/Brokerage Mitigation	Mandatory refresher courses with compliance audits
NSCP16	Information Disclosure/Brokerage Mitigation	Automatic PC locking after idle periods
NSCP17	Information Disclosure/Brokerage Mitigation	Requirement to store sensitive data on local hard disks only
NSCP18	Information Disclosure/Brokerage Mitigation	Enhanced monitoring and regular review of server access

NSCP19	Information Disclosure/Brokerage Mitigation	Personnel action forms required one week before payroll processing
NSCP20	Information Disclosure/Brokerage Mitigation	Protection for information on unattended PCs
NSCP21	Information Disclosure/Brokerage Mitigation	Investigation of server-side encryption capabilities
NSCP22	Information Disclosure/Brokerage Mitigation	Regular review of mainframe access records
NSCP23	Network-Related Threats Mitigation	Prohibition of sensitive information transmission outside HGA
NSCP24	Network-Related Threats Mitigation	Enhanced restrictions for remote access
NSCP25	Network-Related Threats Mitigation	Alternative email system for dial-in users
NSCP26	Network-Related Threats Mitigation	Replacement of current modem pool
NSCP27	Network-Related Threats Mitigation	Encryption for server-to-mainframe communications
NSCP28	Network-Related Threats Mitigation	Enhanced authentication for remote access

Appendix 3: Detailed Network Topology for HGA

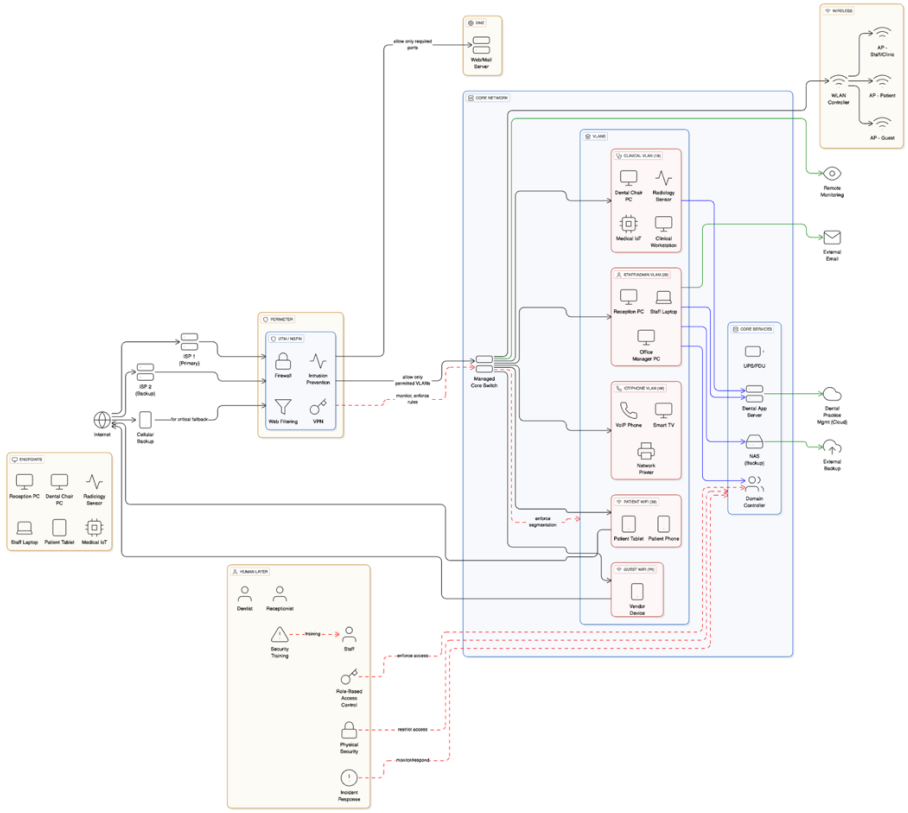


System Description: HGA operates a distributed computer system that processes time and attendance data for federal payroll operations. The system manages sensitive personnel information, including salary data, leave balances, W-2 records, and service dates for agency employees. Our infrastructure consists of personal computers connected through a local area network to a central server that enforces access controls, provides file storage, hosts email services, and executes applications. Time and attendance data entered on workstations undergoes validation on the server before transmission through an inter-agency wide area network to a shared mainframe for payroll processing and electronic funds distribution. The system connects to three external networks: the Internet through a packet-filtering router (email only), an X.25-based inter-agency WAN (authorized applications only), and the public telephone network via modem pool (email access for remote users). Additional capabilities include word processing, data analysis, electronic communications, and management of personnel correspondence and contracting documents.

System Topology: The system follows a three-tier distributed architecture with mixed ownership. The first tier includes our personal computers with local storage and network printers, all connected through the LAN backbone within our security perimeter. The second tier comprises our edge infrastructure: a central LAN server that serves as the primary security enforcement point, an administrator console for privileged system management, a modem pool for remote access, and a router providing filtered Internet connectivity. The third tier consists of external systems beyond our direct control, including the X.25 WAN operated by a commercial telecommunications provider and a multi-agency mainframe owned by another federal agency. The mainframe houses payroll databases and includes its own modem pool for electronic funds transfer. Time and attendance data flows from workstations through our server, across the WAN, to the mainframe, where it generates direct deposits, paychecks, and tax reporting to IRS and state agencies.

Critical Path for Time and Attendance Processing: User PC (data entry) → LAN Server (validation and access control enforcement) → WAN Interface (secure transmission) → X.25 Wide Area Network (inter-agency transport) → Mainframe System (payroll processing and database storage) → Electronic Distribution (direct deposits to employee bank accounts, paychecks, and tax reports to IRS/state agencies)

Appendix 4: Detailed Network Topology (defense-in-depth) for your company



The network topology for BrightSmile Dental Group (Fictional) is intentionally designed using a defense-in-depth strategy that incorporates multiple layers of security controls across the entire clinical environment. This approach ensures that even if one security layer fails, additional protective mechanisms remain in place to safeguard Protected Health Information (PHI), maintain service availability, and meet HIPAA requirements. Central to this architecture is Access Control Security Risk Management, which governs how staff interact with the EHR system, imaging applications, billing software, and administrative tools. This layer includes multi-factor authentication, strong password enforcement, automated session timeout policies, least-privilege access assignments, privileged account monitoring, and quarterly access-control reviews. Additionally, access to sensitive systems is logged through audit trails that record user identity, activity timestamps, system interactions, and administrative changes to ensure accountability and facilitate rapid detection of unauthorized access attempts.

Network Infrastructure Security Risk Management is implemented at the perimeter and internal network layers through a Next-Generation Firewall (NGFW) equipped with intrusion detection and prevention (IDS/IPS), deep packet inspection, anti-malware filtering, geo-blocking, and encrypted VPN tunnels for remote vendor support. This firewall enforces detailed inbound and outbound traffic rules, reducing exposure to unauthorized network probing, brute-force attacks, and malware infiltration. Complementing this is Network Infrastructure Management Security Risk Management, which governs the configuration, maintenance, and monitoring of internal network devices. Managed switches, access control lists (ACLs), secure router configurations, and VLAN segmentation prevent lateral movement within the network by isolating clinical workstations, imaging systems, administrative desktops, servers, and guest devices into

separate security zones. Network segmentation ensures that a breach in one VLAN, such as guest Wi-Fi cannot penetrate into the clinical environment or server infrastructure. Routine switch firmware updates, secure SNMP configurations, disabled unused ports, and continuous log monitoring further strengthen the internal network.

Database Security Risk Management applies to the EHR database, imaging archives, and dental practice-management databases stored in the protected Server VLAN. These systems are protected through AES-256 encryption at rest, TLS 1.3 encryption in transit, granular database user permissions, periodic integrity checks, and strict query-level logging. Automated daily backups, weekly off-site replication, and encrypted cloud disaster recovery snapshots ensure data survivability against ransomware, hardware failure, or environmental disasters. A dedicated backup vault further separates primary and backup data, preventing attackers from compromising both simultaneously. Access to database consoles and administrative panels is restricted to authorized IT personnel using MFA, and all database configuration changes are documented within a change-management process to ensure consistency and reduce misconfiguration risk.

Applications Development Security Risk Management guarantees that all software used by the dental practice, including the EHR system, patient portal, radiography applications, scheduling software, billing systems, and insurance claim processors undergoes ongoing security evaluations. This includes vendor-provided security patches, secure configuration hardening, vulnerability scans, dependency updates, and annual third-party penetration testing. Any custom integrations or add-ons must comply with secure coding standards, undergo code reviews, and be validated before deployment. Application logs are centrally collected and analyzed for unusual authentication patterns, injection attempts, or unauthorized data export activity.

Finally, Wireless Security Risk Management enhances the wireless environment by separating wireless traffic into three isolated SSIDs: secure staff Wi-Fi, clinical device Wi-Fi, and guest Wi-Fi. Each wireless network is configured with WPA3 encryption, rotating complex passphrases, and MAC address filtering for sensitive devices. The clinical Wi-Fi network is restricted to medically approved devices such as tablets, charting tools, and imaging sensors, preventing non-medical equipment from connecting. Rogue access point detection, wireless intrusion detection systems (WIDS), and signal-strength perimeter checks minimize the risk of unauthorized wireless access. Guest Wi-Fi is segmented into a fully isolated VLAN with bandwidth throttling and no access to internal systems, reducing the risk that an infected guest device could impact clinical operations.

END OF DOCUMENT